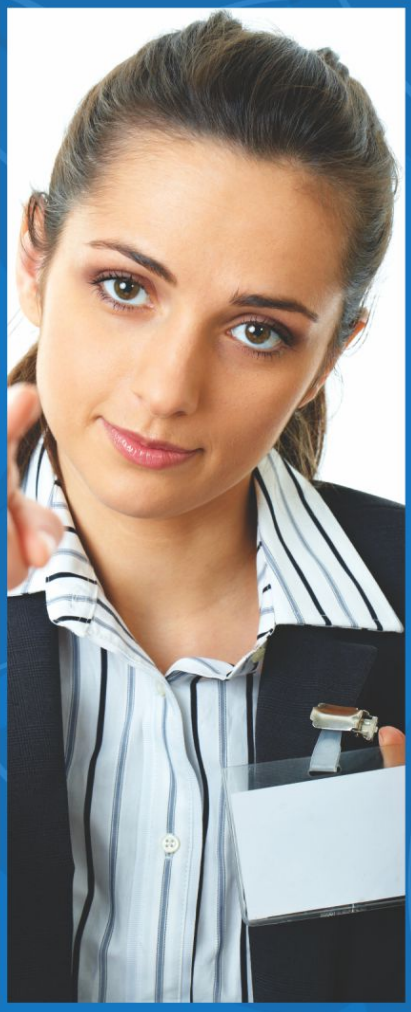
ZigLOCK TCP

Manual de Instalação e Operação



Um produto desenvolvido e fabricado por: Enterplak Produtos Eletrônicos Ltda - CNPJ: 07.013.491/0001-54

Sob licença de

RWTECH

RW Tecnologia Indústria e Comércio Ltda
Centro Empresarial Paulo F. de Toledo, 80
Santa Rita do Sapucaí - MG - CEP: 37540-000
Tel: 35 3471-3172

www.rwtech.com.br

Índice

Antes de Começar....3
Especificações Técnicas....4
Introdução....5
Modelos dos Pontos de Acesso ZigLock TCP....5
Passo a Passo do Conhecimento e Instalação do Controlador ZigLock TCP....6
Passo 1 – Conhecendo o Equipamento....6
a) Meios de Identificação do Usuário....6
b) Menu do Equipamento....7
Passo 2 – Fixando o Suporte do Equipamento à Parede....11
Passo 3 – Fazendo as Ligações Elétricas....12
Passo 4 – Fixando o Equipamento ao Suporte de Fixação....14
Conhecimento da Catraca ZigLock TCP....15
a) Meios de Identificação do Usuário....15
b) Menu do Equipamento....17
Passo a Passo da Instalação, Configuração e Utilização do ZigLock TCP Explorer....19
Passo 1 – Instalando o Software ZigLock TCP Explorer....19
Passo 2 – Cadastrando os Pontos de Acesso....21
Passo 3 – Cadastrando uma Empresa....23
Passo 4 – Cadastrando um Usuário....23
Passo 5 – Cadastrando Bloqueios....27
a) Faixas de Horário....28
b) Falta de Pagamento....29
c) Entrada por Período de Data....30
Passo 6 – Mensagens de Texto (E-mail e SMS)....30
a) Enviando Mensagens de Texto para os Eventos do Sistema....30
b) Enviando Mensagens de Texto para os Eventos de um Usuário Específico. 30
Passo 7 – Relatórios....31
a) Relatórios de Acessos....31
b) Usuários por Ponto de Acesso....32
Passo 8 – Utilitários....32
a) Operadores....32
b) Backup....32
c) Operações em Massa....32
d) Visualizar Log....32
Passo 9 – ZigLock em Rede - Modo Servidor / Modo Estação....33
Notas de Revisão....41

Antes de Começar

Sr. Usuário:

– Leia atentamente este manual e siga corretamente as instruções de instalação e operação. Assim você estará assegurado de que seu equipamento operará em suas melhores condições de uso.

– Em caso de instalação do equipamento sem as precauções citadas, qualquer troca de peças e manutenção será cobrada.

– A ligação do aparelho à rede elétrica (110/220V) e aos acionamentos externos deve ser efetuada conforme este manual. A ligação errada da rede elétrica ou das demais conexões podem causar danos ao aparelho, não assegurados pela garantia.

– Solicite a instalação a um profissional habilitado.

Antes de instalar seu equipamento, tome as seguintes precauções:

– Verifique se o local é adequado, se o ambiente é coberto, protegido contra água, sol, poeira e outros que podem danificar seu equipamento, pois este equipamento não é adequado para instalação em ambientes externos.

– Evite instalá-lo em ambientes nos quais os usuários possuam, por algum motivo, dedos sujos ou com digitais prejudicadas por produtos químicos, dentre outros.

Observações	*Há um número reduzido de pessoas que não possui digitais com qualidade suficiente para identificação (digitais muito úmidas ou secas, desgastadas, etc.). Assim, para esses casos, o produto oferece a identificação através de cartão de proximidade ou teclado (digitação de matrícula e senha) para o controle de acesso desses usuários.* *Qualquer sistema de identificação biométrica possui taxas de erros FRR (falsa rejeição) e FRA (falso aceite), que devem ser consideradas na aplicação final do produto.*

ANATEL

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

ATENÇÃO	*Este documento pode conter imprecisões técnicas ou erros tipográficos.* *A RW Tecnologia reserva-se o direito de fazer aprimoramentos e/ou alterações no produto aqui descrito a qualquer momento sem aviso prévio.* *Algumas telas ou recursos do software gerenciador ZigLock TCP Explorer, aqui apresentados, podem não coincidir exatamente com as telas atuais do software.*

Especificações Técnicas

PEÇAS	ESPECIFICAÇÕES
Processador	ARM7TDMI-S 72MHz
Memória de Sistema	Cartão SD
Display	Alfanumérico de LCD (2 linhas x 16 colunas)
Identificação	1. Matrícula e senha numéricas
	2. Cartão de proximidade RFID 125kHz
	3. Leitura biométrica por digital (modelos BIOCARDs)
Comunicação	Protocolo TCP/IP via *Ethernet* de 100Mbps
Teclado	Numérico com funções de navegação
Portas e Conectores	1 conector USB 2.0
	1 conector contendo*: • 1 saída para acionamento de fechadura • 1 saída para acionamento auxiliar • 1 entrada de alimentação 12V DC • 1 entrada de alimentação de carga • 2 entradas para botoeira e/ou sensor de porta aberta (local e/ou intertravamento), nomeadas Entrada 1 e Entrada 2.
Alimentação	Fonte de 12V 1A (12W)

** Disponível somente nos Controladores ZigLock TCP.*

Introdução

O *Sistema ZigLock TCP* foi concebido para permitir o efetivo controle do acesso de pessoas, a fim de auxiliar a sua proteção física e patrimonial.

Este manual apresenta o *Sistema ZigLock TCP* com seus dois componentes:

1. **Pontos de Acesso *ZigLock TCP*** (*Catraca ZigLock TCP* e *Controlador ZigLock TCP*): atuam como interface de identificação do usuário, controlando os acessos físicos.
2. **Software *ZigLock TCP Explorer*** (instalado no PC): permite o cadastro dos usuários e o gerenciamento dos eventos de acesso gerados pelos pontos de acesso.

A comunicação entre eles se dá através da *Ethernet* de 100Mbps, utilizando o protocolo TCP (comunicação segura) na camada de transporte do protocolo TCP/IP.

Por usar TCP/IP via *Ethernet*, todas as vantagens existentes nesse tipo de comunicação se fazem presentes: segurança, agilidade, possibilidade de utilizar a própria rede local (LAN) da empresa, possibilidade de utilizar VPN para comunicação através da internet com outra LAN (alcance global), grande familiaridade de profissionais de TI com a tecnologia (*Ethernet* + TCP/IP), possibilidade de testar se o dispositivo está configurado corretamente na rede utilizando o comando “ping”, etc.

Modelos dos Pontos de Acesso *ZigLock TCP*

Os modelos atualmente comercializados dos pontos de acesso *ZigLock TCP* são:

- ***Controlador ZigLock TCP CARD***: modelo do controlador de acesso com identificação por cartão de proximidade (*CARD*).
- ***Controlador ZigLock TCP BIOCARD 480***: modelo do controlador de acesso com identificação por biometria (*BIO*) e cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 480 digitais.
- ***Controlador ZigLock TCP BIOCARD 1500***: modelo do controlador de acesso com identificação por biometria (*BIO*) e cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 1500 digitais.
- ***Catraca ZigLock TCP CARD***: modelo da catraca com identificação por cartão de proximidade (*CARD*).
- ***Catraca ZigLock TCP BIOCARD 480***: modelo da catraca com identificação por biometria (*BIO*) e por cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 480 digitais.
- ***Catraca ZigLock TCP BIOCARD 1500***: modelo da catraca com identificação por biometria (*BIO*) e por cartão de proximidade (*CARD*), possuindo capacidade para armazenar até 1500 digitais.

Observação	*Todos os modelos, tanto do controlador quanto da catraca, permitem identificação também pelo teclado disponível no próprio equipamento.*

Passo a Passo do Conhecimento e Instalação do *Controlador ZigLock TCP*

Passo 1 – Conhecendo o Equipamento

Figura 1

a) Meios de Identificação do Usuário

Os usuários serão identificados pelo *Controlador ZigLock TCP* conforme leitores vistos na **Figura 1** (itens 1, 2 e 3).

Todos os modelos do controlador de acesso *ZigLock TCP* possuem leitor de cartões de proximidade (*RFID*, na forma de chaveiros ou cartões).

Observação	*Dentro destes identificadores, há um chip eletrônico com número único, funcionando como uma identidade digital. Ao ser aproximado à sua leitora, o chip é alimentado e envia, ao aparelho, seu número; por isso, não utiliza pilhas ou baterias.*

Por não haver contato direto (atrito) do cartão com a leitora, o sistema oferece baixo índice de manutenção, bem como maior tecnologia e segurança com relação a sistemas similares de códigos de barras e tarjas magnéticas.

Os cartões podem ser adquiridos diretamente com seu representante e são personalizáveis de acordo com a sua necessidade.

O modelos *ZigLock TCP BIOCARD* trabalha também fazendo a leitura das digitais dos usuários, que não são iguais nem mesmo entre dois dedos de uma mesma pessoa. Para agilizar a identificação, são capturados os pontos únicos em uma digital, chamados minúcias.

O produto torna-se de grande utilidade para o usuário, pois não há o problema do esquecimento de cartões, uma vez que ele pode garantir seu acesso pela identificação da própria impressão digital.

Os benefícios à empresa também são muito interessantes: economia na aquisição e reposição de crachás, bem como a eliminação de fraudes no controle de acesso (garante que o acesso do usuário só será registrado com a presença física do mesmo).

O teclado do equipamento (item 1 da **Figura 1**) possui, também, a função de permitir acesso aos usuários, além de permitir o acesso a funções especiais, conforme ilustra a **Figura 2**.

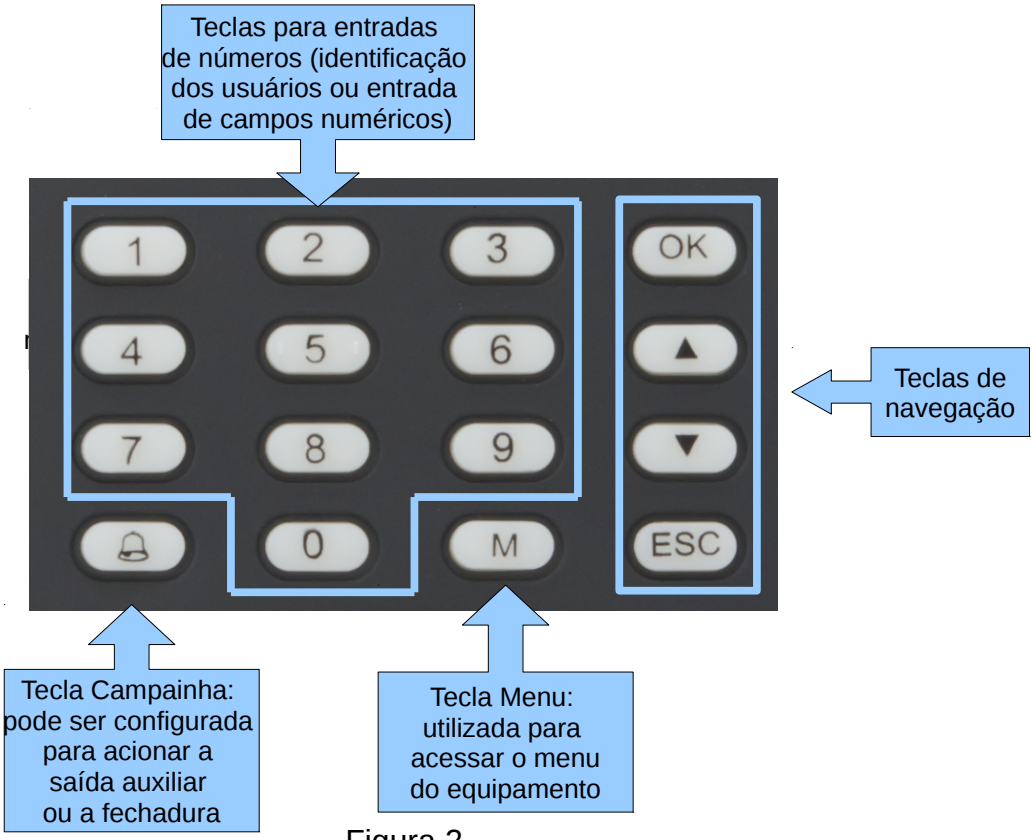


Figura 2

Observação	*Para facilitar a instalação e teste de um equipamento novo, que não tenha nenhum usuário cadastrado, pode-se digitar "123" e a tecla "OK" para liberar o acesso (acionar o fecho ou fechadura). Após o cadastro do primeiro usuário no ponto de acesso, não é mais possível liberar o acesso dessa forma.*

b) Menu do Equipamento

Através do menu do equipamento (**Figura 3**), pode-se: (1) realizar diversas configurações do funcionamento e ajustes do equipamento, (2) visualizar informações a respeito da versão do *firmware* e (3) colocar o equipamento em modo de gravação para ser possível atualizar o *firmware* do equipamento. O menu se encontra organizado da seguinte forma:

1. Configuração do TCP/IP

Menu de leitura e configuração relacionadas à comunicação TCP/IP.

1.1. Endereço IP

Permite ler e atualizar o endereço IP do equipamento da rede. Exemplo: 10.0.0.123 (em rede classe A), 172.16.0.123 (em rede classe B) ou 192.168.0.123 (em rede classe C).

1.2. Máscara de Rede

Permite ler e atualizar a máscara de sub-rede utilizada na rede onde o equipamento está configurado. Exemplo: 255.0.0.0 (padrão da rede classe A), 255.255.0.0 (padrão da rede classe B) ou 255.255.255.0 (padrão da rede classe C).

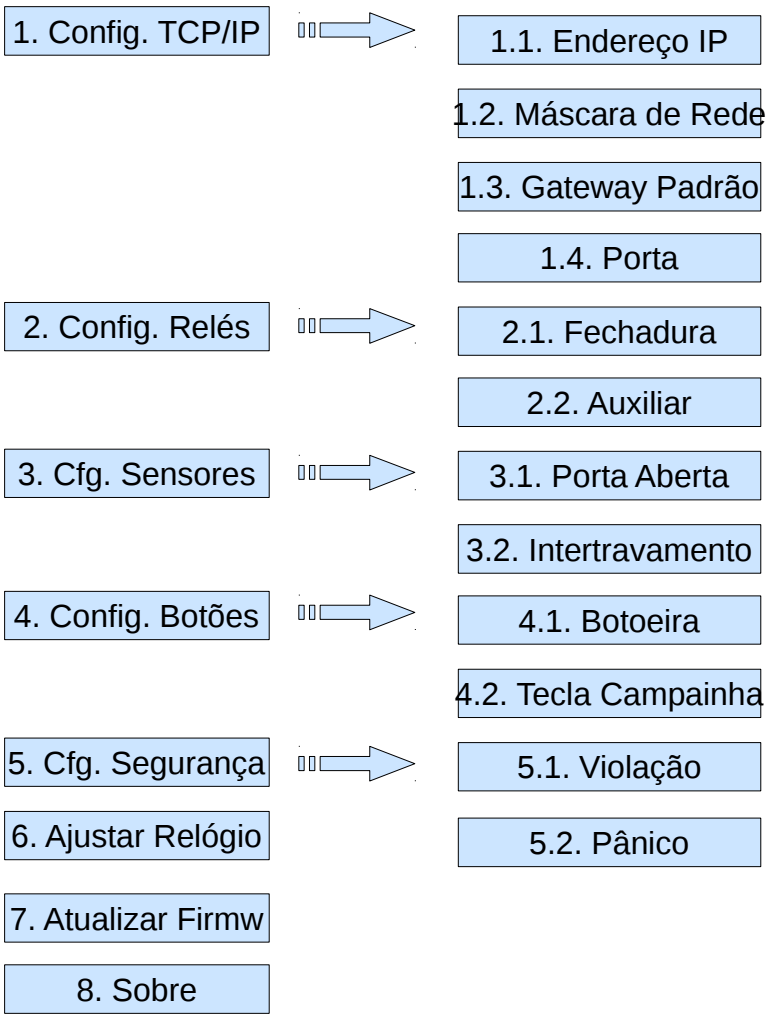


Figura 3

1.3. *Gateway* Padrão

Permite ler e atualizar o *gateway* padrão utilizado na rede, o qual é o *host* destino pra onde o equipamento deve encaminhar os pacotes caso o destinatário não esteja visível na rede local. Uma vez encaminhado um pacote TCP/IP ao *gateway* padrão, ele se encarrega de encaminhá-lo para fora da rede local, buscando entregá-lo ao destinatário.

1.4. Porta

Permite ler e atualizar a porta utilizada para realizar a comunicação com o PC. A porta de rede é muito importante, pois pode ser utilizada para encaminhar pacotes vindos da internet diretamente ao equipamento dentro da rede local (configuração feita no roteador), além de ser utilizado em configurações de segurança e prioridades dentro das redes. É importante verificar que nenhum *firewall*, do PC onde está instalado o aplicativo *ZigLock TCP Explorer* ou outro equipamento que possa bloquear pacotes em nível de porta, esteja bloqueando a porta utilizada pelo equipamento.

2. Configuração dos Relés

Menu de configuração do funcionamento dos 2 relés (saídas) disponíveis no equipamento. Através deste menu, é possível: (1) selecionar se o dispositivo é NA

(normalmente aberto) ou NF (normalmente fechado), sendo possível configurar a largura de pulso que será dada ao acionar o relé (modo pulsar) ou (2) selecionar se o dispositivo funcionará no modo comutar, onde o relé é invertido (fechado/aberto) a cada acionamento; este modo (comutar) pode ser utilizado para ligar/desligar lâmpadas, por exemplo.

Observação	*O tempo utilizado para configurar o pulso no menu está em milissegundos (ms), ou seja, se for preciso configurar um pulso grande, de 15 segundos, por exemplo, é necessário digitar 15000 (15000 milissegundos = 15 segundos).*

2.1. Fechadura

Permite configurar o relé da fechadura, o qual será utilizado para liberar o acesso do usuário ao local controlado pelo ponto de acesso. Esse relé pode ser acionado através dos seguintes estímulos: (1) identificação de um usuário com acesso liberado (estímulo padrão), (2) pressionamento de uma botoeira (acionada por um porteiro, por exemplo) ou (3) pressionamento da *Tecla Campainha* do próprio equipamento.

Observação	*Os estímulos (2) e (3) devem ser ativados e configurados através do próprio menu para funcionarem.*

2.2. Auxiliar

Permite configurar o relé auxiliar do equipamento. Esse relé auxiliar pode ser utilizado para acionar um dos diversos dispositivos, externos ao equipamento (não inclusos), possíveis; por exemplo: lâmpadas, alarmes e circuitos de segurança [para avisar o dono da empresa ou, diretamente, a polícia da ocorrência de um assalto (pânico), por exemplo].

O relé auxiliar ou **saída auxiliar**, como também é tratado, pode ser acionado através dos seguintes estímulos: (1) pressionamento de uma botoeira, (2) pressionamento da *Tecla Campainha* do próprio equipamento, (3) ocorrência da violação do equipamento (retirada do equipamento de seu suporte), (4) ocorrência de pânico (identificado pela digitação de um dígito qualquer a mais no final da senha durante a identificação do usuário por matrícula e senha ou por um dedo marcado como dedo de pânico) ou (5) estouro do tempo (*timeout*) de espera para que a porta seja fechada.

Observação	*Todos os estímulos devem ser ativados e configurados através do próprio menu para funcionarem.*

3. Configuração dos Sensores

Menu de configuração de possíveis sensores de porta aberta ligados ao equipamento através das 2 entradas disponíveis (*Entrada 1* e *Entrada 2*).

3.1. Porta Aberta

Permite configurar um sensor de porta aberta local ao equipamento com o uso de uma das entradas (*Entrada 1* ou *Entrada 2*), que deve estar disponível para isso. Com esse sensor de porta aberta, é possível acionar o relé auxiliar se a porta não for fechada pelo tempo configurado no menu (identificado como *timeout*), sendo possível soar um alarme ou ligar uma lâmpada de alerta, por exemplo, avisando que a porta foi esquecida aberta e que deve ser fechada.

3.2. Intertravamento

Permite configurar um sensor de porta aberta ligado à porta acionada por outro

ponto de acesso. Com esse recurso, é possível bloquear o acesso de um usuário caso ele tenha esquecido de fechar a outra porta de um corredor, por exemplo, forçando-o a fechar primeiro a outra porta para depois conseguir a liberação do acesso. Esse tipo de bloqueio é conhecido como intertravamento ou gaiola de proteção.

4. Configuração dos Botões

Menu de configuração da botoeira e da *Tecla Campainha* do equipamento.

4.1. Botoeira

Permite configurar o uso de uma botoeira ligada a uma das entradas (*Entrada 1* ou *Entrada 2*) que esteja disponível no equipamento para: (1) acionar a fechadura ou (2) acionar o relé auxiliar.

4.2. Tecla Campainha

Permite configurar o uso da *Tecla Campainha*, do próprio equipamento, para: (1) acionar a fechadura ou (2) acionar o relé auxiliar.

5. Configuração de Segurança

Menu de configuração dos recursos relacionados à segurança disponíveis no equipamento.

5.1. Violação

Permite configurar se o relé auxiliar será ou não acionado durante a ocorrência da violação do equipamento. A violação do equipamento se dá quando ele é retirado de seu suporte enquanto está ligado, momento em que uma pessoa mal-intencionada pode tentar acionar a fechadura ou o relé auxiliar de maneira forçada, pois terá acesso às conexões do equipamento.

5.2. Pânico

Permite configurar se o relé auxiliar será ou não acionado durante a ocorrência de pânico sinalizada pelo usuário. Essa sinalização de pânico é realizada com: (1) a digitação de um dígito qualquer a mais no final da senha durante a identificação do usuário por matrícula e senha ou (2) a identificação do usuário pela digital marcada como digital de pânico.

Esse recurso, conhecido como pânico, é utilizado para sinalizar para o sistema que está ocorrendo algum problema com o usuário (está sendo assaltado, sequestrado, passando mal, quer que alguém do RH lhe procure para uma conversa ou precisou sair às pressas, por exemplo). Ao configurar a saída auxiliar para acionar um circuito externo (não incluso), pessoas ou equipes próprias para resolver os problemas de pânico podem ser avisadas automaticamente pelo próprio sistema.

ATENÇÃO	*1. Por motivos de segurança, para que um assaltante não perceba que o usuário está sinalizando pânico, por exemplo, mesmo que a saída auxiliar seja acionada no momento, nada além da mensagem de liberação ou bloqueio de acesso será exibida no display do equipamento.* *2. A sinalização de pânico não altera as prioridades de acesso do usuário, ou seja, o acesso é controlado normalmente, podendo ser liberado ou bloqueado.*

6. Ajustar Relógio

Permite configurar o relógio do equipamento automaticamente (quando o PC está *online*) ou manualmente.

7. Atualizar o *Firmware*

Permite colocar o equipamento em modo de atualização de *firmware*. Para isso, é necessário um cabo USB e o arquivo com o conteúdo do *firmware* a ser atualizado no equipamento.

Após colocar o *firmware* em modo de atualização, quando o *display* fica com o fundo apagado, os seguintes passos devem ser executados para realizar a atualização do equipamento de fato:

1. Retire o equipamento de seu suporte, sem desligá-lo, para ter acesso à porta USB do equipamento.
2. Conecte o cabo USB (macho x macho) no equipamento e no PC.
3. Ao aparecer uma nova unidade USB de armazenamento chamada “RW ZigLock”, apague o arquivo “firmware.bin” que estará nela.
4. Copie a versão mais atual do *firmware* (ex.: “CONTROLADOR_ZIGLOCK_TCP-v3.00.bin”) para a mesma unidade USB.
5. Mande ejetar a unidade USB (“RW ZigLock”) e desconecte o cabo USB logo em seguida.

Observação	*Neste momento, o equipamento será reiniciado e começará a executar o novo firmware.*

6. Recoloque o equipamento em seu suporte o quanto antes, pois o *firmware* novo ficará sinalizando violação enquanto isso não for feito.

7. Sobre

Permite visualizar a identificação do equipamento, incluindo seu nome, versão e momento da compilação do *firmware* (através do código hexadecimal exibido).

Passo 2 – Fixando o Suporte do Equipamento à Parede

O suporte de fixação (acompanha o produto), que pode ser visto na **Figura 4**, é útil para manter o equipamento fixo e travado na parede, além de garantir o seu correto funcionamento.

Os furos do suporte (indicados pelas setas na **Figura 4**) são aqueles que serão fixados na parede através de parafusos. Estes furos “casam” exatamente com o tamanho e localização dos parafusos de caixas padrões 4x2; desta forma, é possível instalar o equipamento sem, ao menos, fazer furos na parede.

Observe a **Figura 4** para a devida posição do suporte. Puxe os fios do conduíte para que passem por dentro da cavidade do suporte antes de fixá-lo à caixa 4x2.

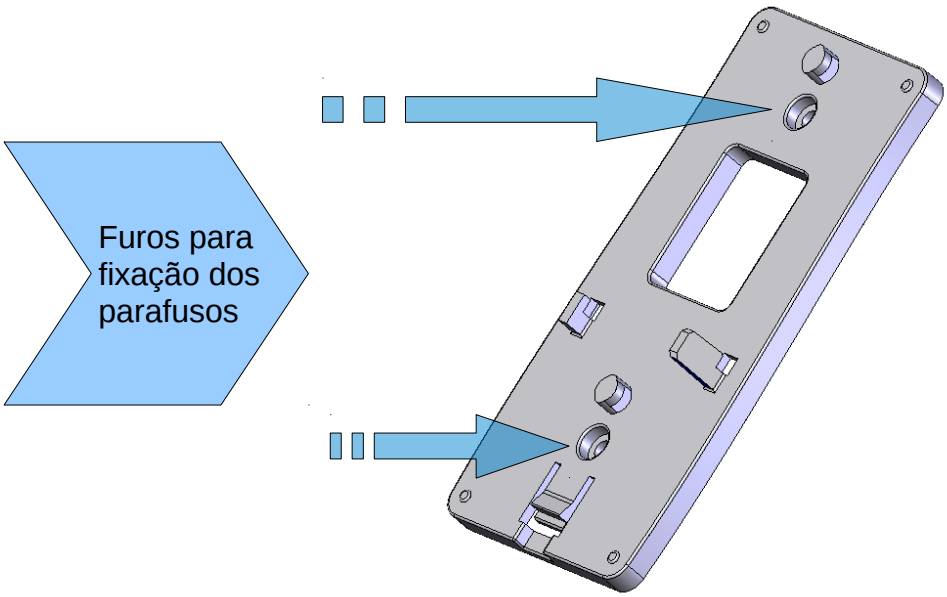


Figura 4

Passo 3 – Fazendo as Ligações Elétricas

Todos os fios de ligação do equipamento são colocados em sua parte traseira, conforme visto na **Figura 5**.

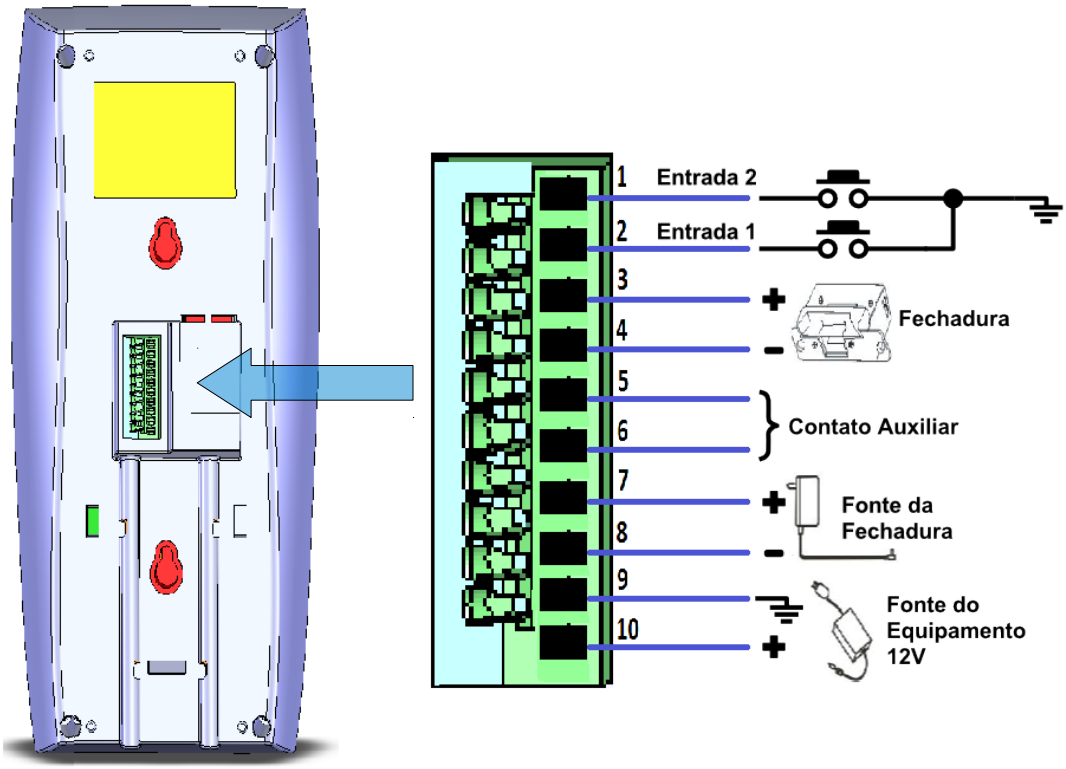


Figura 5

– Pino 1: destinado à ligação de (1) uma botoeira, possibilitando a abertura da fechadura sem que haja uma identificação (isso também pode ser feito utilizando a

Tecla Campainha, do teclado do próprio equipamento), (2) um sensor de porta aberta local, possibilitando acionar um alarme ou acender uma luz se a porta ficar aberta após o tempo de espera configurado ou (3) um sensor de porta aberta remoto, possibilitando bloquear o acesso a um determinado controlador se a porta controlada por outro controlador ainda estiver aberta (intertravamento). Todos esses recursos devem ser NA (normalmente abertos).

Observação	*Considere estas mesmas características e possibilidades para a "Entrada 1" (pino 2); com estas 2 entradas (Entrada 1 e Entrada 2), pode-se ligar uma botoeira e um sensor de porta aberta, ao mesmo tempo, no equipamento, por exemplo.*

– Pinos 3 e 4: destinados à ligação de um fecho ou fechadura (não inclusos), configuráveis em NA (normalmente abertos) ou NF (normalmente fechados) pelo menu do próprio equipamento. Dependendo da configuração, realizada no menu do próprio equipamento, e do acionamento realizado, as seguintes conexões são estabelecidas:
  – Pino 7 ligado ao Pino 3.
  – Pino 8 ligado ao Pino 4.

ATENÇÃO	*Este contato suporta fechaduras de até 1,5 A. Não exceda este valor!*

Caso a fechadura seja do tipo de alimentação contínua (DC), recomenda-se a utilização de um diodo *FR107* (incluso) para evitar danos ao sistema. Para este caso, siga o esquema da **Figura 6.**

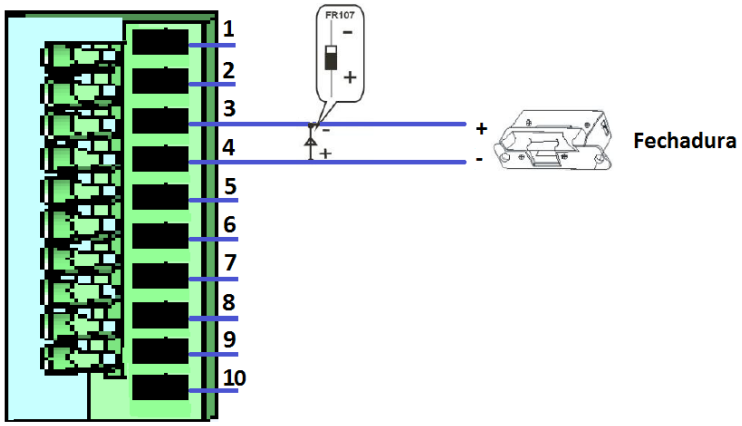


Figura 6

– Pinos 5 e 6: estes são pinos do relé auxiliar, o qual pode ser utilizado para ligar uma lâmpada, acionar uma campainha, ativar um alarme, acionar um determinado circuito externo (todos não inclusos), dentre outros. De acordo com a configuração feita pelo menu do próprio equipamento, esta saída auxiliar (relé) pode ser configurada (1) como NA ou NF, com largura de pulso configurável ou (2) em modo comutar, onde cada acionamento faz com que o contato seja invertido (para ligar e desligar uma lâmpada, por exemplo). A funcionalidade de ligar ou desligar uma lâmpada pode ser útil nos casos onde o equipamento é instalado exatamente no lugar do interruptor da lâmpada, já que o equipamento possui um suporte para fixação em caixas elétricas 4x2. Vide o **Passo 2 – Fixando o Suporte do Equipamento à Parede** para mais detalhes neste sentido.
– Pinos 7 e 8: destinados à ligação da fonte de alimentação compatível com o fecho ou fechadura instalado. Consulte o fabricante desses dispositivos para escolher corretamente uma fonte compatível.

ATENÇÃO	***Não** utilize a fonte do equipamento (pinos 9 e 10) para alimentar estes pinos.*

– Pinos 9 e 10: nestes pinos, é ligada a fonte de alimentação do equipamento.

Passo 4 – Fixando o Equipamento ao Suporte de Fixação

Uma vez com o suporte fixado e os fios conectados ao aparelho, siga a **Figura 7** para o devido encaixe do equipamento ao suporte.

Encaixe os pinos do suporte às cavidades da parte posterior do equipamento, conforme a **Figura 7**, e empurre o equipamento para baixo; isso fará com que ele fique travado ao suporte, segurando-o à parede. Isto se dá por um sistema de “click” que trava uma lingueta do suporte a um orifício do equipamento.

Quando for necessário retirar o equipamento da parede: (1) insira uma chave de fenda entre o equipamento e o suporte para liberar o “click”, (2) empurre o equipamento para cima e (3) puxe o equipamento para frente.

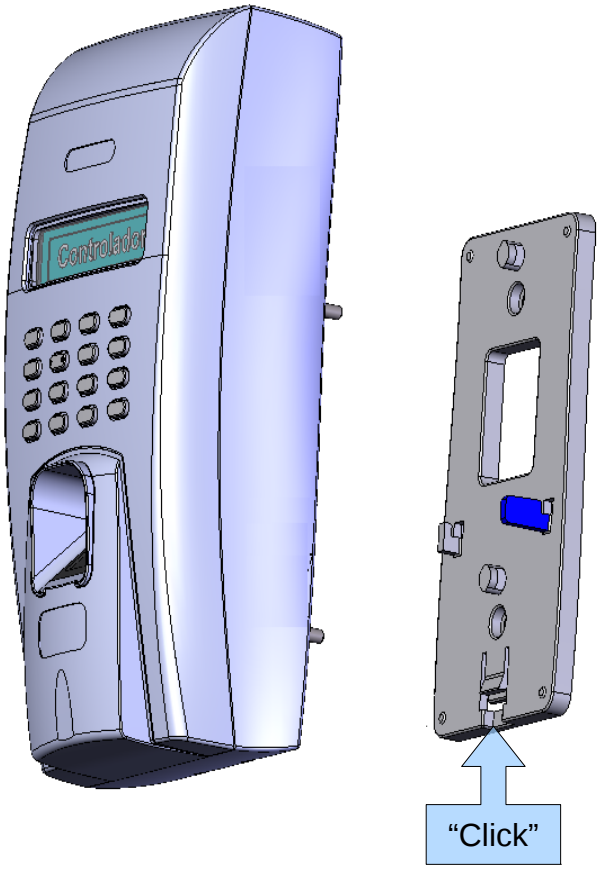


Figura 7

Conhecimento da *Catraca ZigLock TCP*

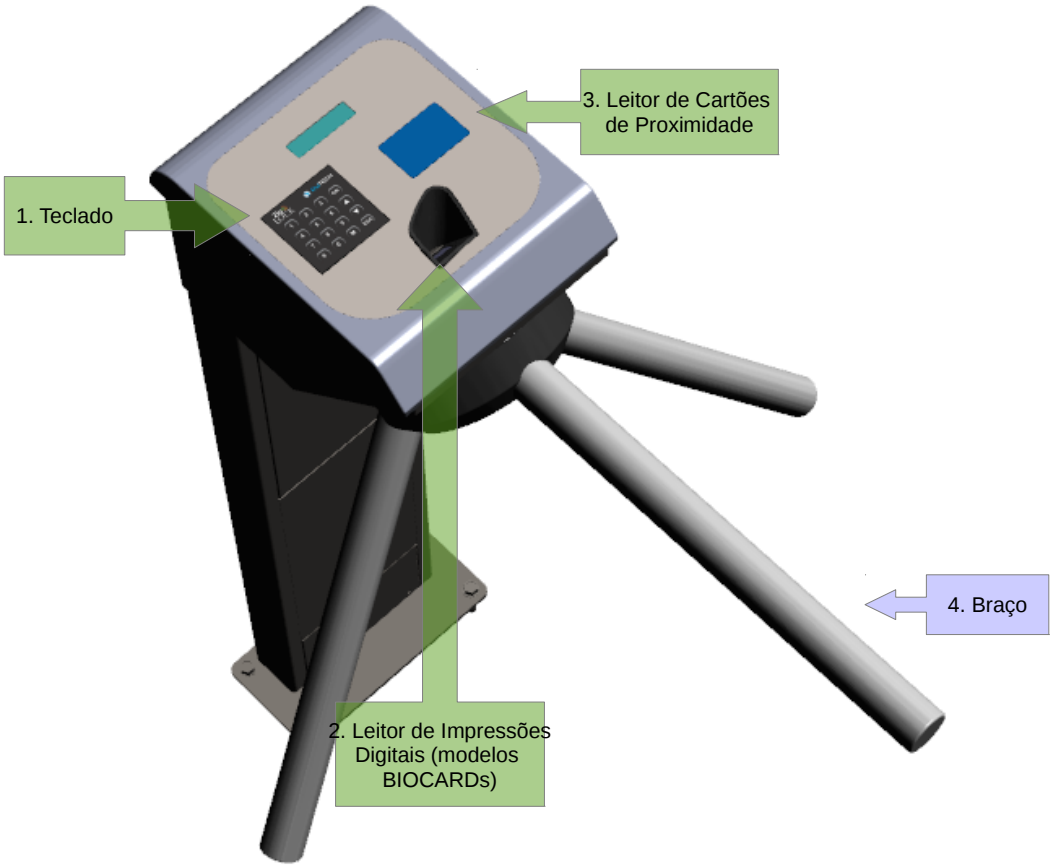


Figura 8

a) Meios de Identificação do Usuário

Os usuários serão identificados pela *Catraca ZigLock TCP* conforme leitores vistos na **Figura 8** (itens 1, 2 e 3).

Todos os modelos da *Catraca ZigLock TCP* possuem leitor de cartões de proximidade (*RFID*, na forma de chaveiros ou cartões) e teclado.

Observação	*Dentro destes identificadores, há um chip eletrônico com número único, funcionando como uma identidade digital. Ao ser aproximado à sua leitora, o chip é alimentado e envia, ao aparelho, seu número; por isso, não utiliza pilhas ou baterias.*

Por não haver contato direto (atrito) do cartão com a leitora, o sistema oferece baixo índice de manutenção, bem como maior tecnologia e segurança com relação a sistemas similares de códigos de barras e tarjas magnéticas.

Os cartões podem ser adquiridos diretamente com seu representante e são personalizáveis de acordo com a sua necessidade.

Os modelos *ZigLock TCP BIOCARD 480* e *ZigLock TCP BIOCARD 1500* trabalham também fazendo a leitura das digitais dos usuários, que não são iguais nem mesmo entre dois dedos de uma mesma pessoa. Para agilizar a identificação, são capturados os pontos únicos em uma digital, chamados minúcias.

O produto torna-se de grande utilidade para o usuário, pois não há o problema do

esquecimento de cartões, uma vez que ele pode garantir seu acesso pela identificação da própria impressão digital.

Os benefícios à empresa também são muito interessantes: economia na aquisição e reposição de crachás, bem como a eliminação de fraudes no controle de acesso (garante que o acesso do usuário só será registrado com a presença física do mesmo).

O teclado do equipamento possui também a função de permitir acesso aos usuários, além de permitir também o acesso a funções especiais, conforme ilustra a **Figura 10**.

Teclas para entradas de números (identificação dos usuários ou entrada de campos numéricos)

Figura 9

Observação	*Para facilitar a instalação e teste de um equipamento novo, que não tenha nenhum usuário cadastrado, pode-se digitar "123" e a tecla "OK" para liberar o acesso. Após o cadastro do primeiro usuário no ponto de acesso, não é mais possível liberar o acesso dessa forma.*

b) Menu do Equipamento

Através do menu do equipamento (**Figura 10**), pode-se: (1) realizar alguns ajustes do equipamento, (2) visualizar informações a respeito da versão do *firmware* e (3) colocar o equipamento em modo de gravação para ser possível atualizar o seu *firmware*.

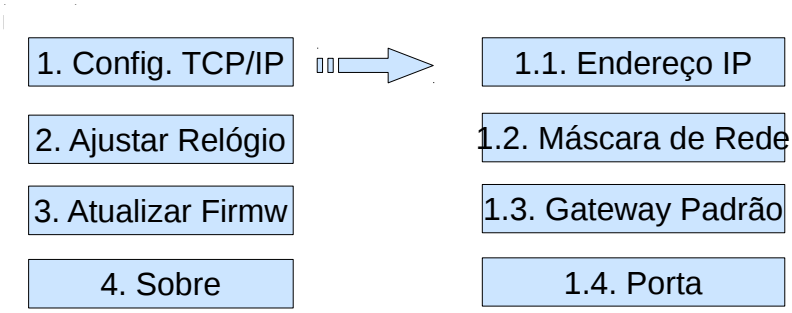


Figura 10

1. Configuração do TCP/IP

Menu de leitura e configuração relacionadas à comunicação TCP/IP.

1.1. Endereço IP

Permite ler e atualizar o endereço IP do equipamento da rede. Exemplo: 10.0.0.123 (em rede classe A), 172.16.0.123 (em rede classe B) ou 192.168.0.123 (em rede classe C).

1.2. Máscara de Rede

Permite ler e atualizar a máscara de sub-rede utilizada na rede onde o equipamento está configurado. Exemplo: 255.0.0.0 (padrão da rede classe A), 255.255.0.0 (padrão da rede classe B) ou 255.255.255.0 (padrão da rede classe C).

1.3. *Gateway* Padrão

Permite ler e atualizar o *gateway* padrão utilizado na rede, o qual é o *host* destino pra onde o equipamento deve encaminhar os pacotes caso o destinatário não esteja visível na rede local. Uma vez encaminhado um pacote TCP/IP ao *gateway* padrão, ele se encarrega de encaminhá-lo para fora da rede local, buscando entregá-lo ao destinatário.

1.4. Porta

Permite ler e atualizar a porta utilizada para realizar a comunicação com o PC. A porta de rede é muito importante, pois pode ser utilizada para encaminhar pacotes vindos da internet diretamente ao equipamento dentro da rede local (configuração feita no roteador), além de ser utilizado em configurações de segurança e prioridades dentro das redes. É importante verificar que nenhum *firewall*, do PC onde está instalado o aplicativo *ZigLock TCP Explorer* ou outro equipamento que possa bloquear pacotes em nível de porta, esteja bloqueando a porta utilizada pelo equipamento.

2. Ajustar Relógio

Permite configurar o relógio do equipamento automaticamente (quando o PC está *online*) ou manualmente.

3. Atualizar o *Firmware*

Permite colocar o equipamento em modo de atualização de *firmware*. Para isso, é necessário um cabo USB e o arquivo com o conteúdo do *firmware* a ser atualizado no equipamento.

Após colocar o *firmware* em modo de atualização, quando o *display* fica com o fundo apagado, os seguintes passos devem ser executados para realizar a atualização do equipamento de fato:

1. Conecte o cabo USB (macho x macho), ligado à placa do equipamento, no PC.
2. Ao aparecer uma nova unidade USB de armazenamento chamada “RW ZigLock”, apague o arquivo “firmware.bin” que estará nela.
3. Copie a versão mais atual do *firmware* (ex.: “CATRACA_ZIGLOCK_TCP-v3.00.bin”) para a mesma unidade USB.
4. Mande ejetar a unidade USB (“RW ZigLock”) e desconecte o cabo USB do PC logo em seguida.

Observação	*Neste momento, o equipamento será reiniciado e começará a executar o novo firmware.*

4. Sobre

Permite visualizar a identificação do equipamento, incluindo seu nome, versão e momento da compilação do *firmware* (através do código hexadecimal exibido).

Passo a Passo da Instalação, Configuração e Utilização do *ZigLock TCP Explorer*

Passo 1 – Instalando o Software *ZigLock TCP Explorer*

Este software deve ser instalado no PC que será utilizado para o gerenciamento do sistema, sendo, preferencialmente, de uso único para este fim.

Para uma utilização de desempenho satisfatório, as configurações recomendadas para este PC são:

– Processador *Intel® Core™ i3* ou superior.

– 4GB de memória RAM ou superior.

– Resolução de tela de 1024 x 768 pixels ou superior.

É fundamental que a conta utilizada para a instalação tenha permissões de administrador para que tudo funcione corretamente.

A instalação do *ZigLock TCP Explorer* pode ser feita através do CD-ROM que acompanha o produto, seguindo os passos abaixo:

1. Execute o arquivo “instalar ZigLock TCP Explorer.exe”.

Observação	*Se for exibida a tela “Deseja permitir que o programa de um fornecedor desconhecido faça alterações neste computador?”, clique em “Sim”.*

2. Clique em “OK” na tela “Selecionar Idioma do Programa de Instalação”.

Observação	*Se estiver selecionado um idioma diferente de “Português (Brasil)”, é recomendado que ele seja selecionado antes de clicar em “OK”.*

3. Clique em “Avançar >” na tela “Bem-vindo ao Assistente de Instalação de ZigLock TCP”.

4. Clique em “Avançar >” na tela “Escolha a Pasta de destino”.

Observação	*Se quiser instalar em algum outro lugar específico, especifique-o no campo editável no centro da tela.*

5. Clique em “Avançar >” na tela “Selecionar a Pasta do Menu Iniciar”.

Observação	*Se quiser utilizar um outro nome para identificar o ZigLock TCP Explorer, especifique-o no campo editável no centro da tela.*

6. Clique em “Instalar” na tela “Pronto para Instalar”.

Observação	*Se você personalizou o local de instalação ou o nome de identificação do aplicativo no Menu Iniciar, confira as informações exibidas na tela (“Local de destino” e “Pasta do Menu Iniciar”) antes de clicar em “Instalar”; caso haja algo errado, clique em “< Voltar” para corrigir e siga novamente os passos até voltar nesta tela.*

7. Aguarde a realização da instalação na tela “Instalando”.

8. Clique em “OK” na tela “Seleccione o Idioma do Assistente de Instalação” que será exibida.

Observação	*Se estiver selecionado um idioma diferente de “Português (Portugal)”, é recomendado que ele seja selecionado antes de clicar em “OK”.*

9. Clique “Seguinte >” na tela “Bem-vindo ao Assistente de Instalação do Firebird”.

10. Clique em “Aceito o contrato” e em “Seguinte >” na tela “Contrato de licença”.

11. Clique em “Seguinte >” na tela “Informação”.

12. Clique em “Seguinte >” na tela “Seleccione a localização de destino”.

Observação	*Se quiser instalar em algum outro lugar específico, especifique-o no campo editável no centro da tela.*

13. Clique em “Seguinte >” na tela “Seleccione os componentes”.

14. Marque a opção “Não criar nenhuma pasta no Menu Iniciar” e clique em “Seguinte >” na tela “Seleccione a pasta do Menu Iniciar”.

15. Marque a opção “Copiar a biblioteca do cliente Firebird para a pasta de <system>?” na tela “Seleccione tarefas adicionais” e clique em “Seguinte >” (**Figura 11**).

ATENÇÃO	*Não modifique as opções pré-selecionadas.*

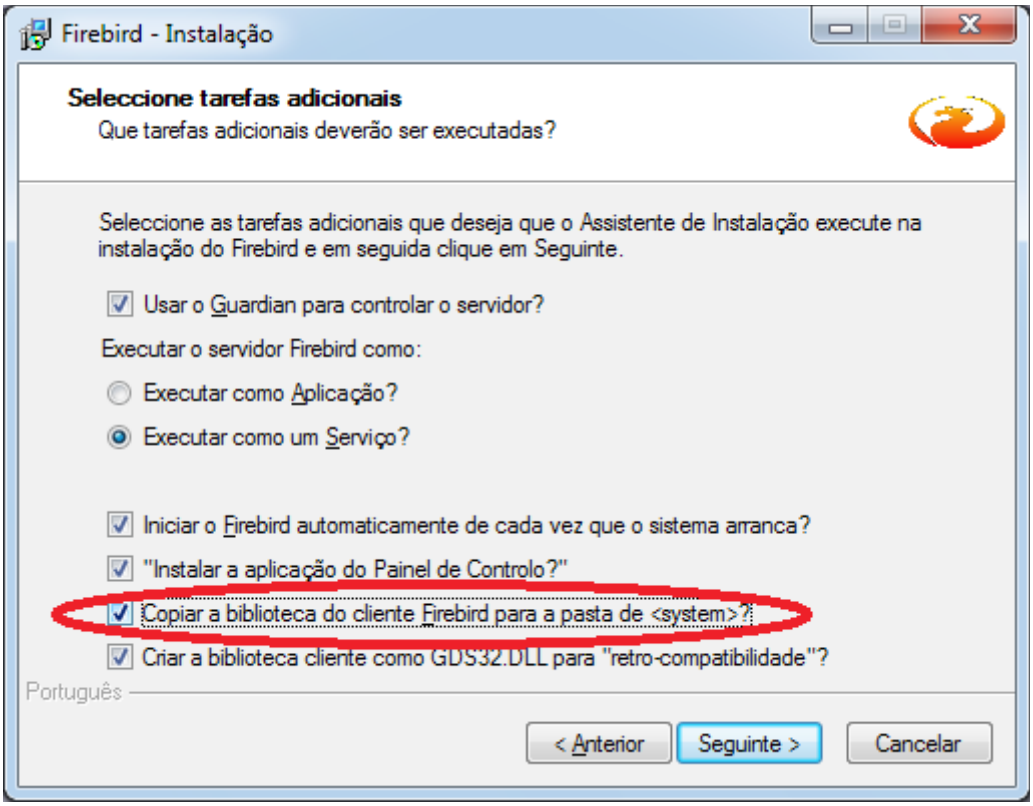

Firebird - Instalação
Seleccione tarefas adicionais
Que tarefas adicionais deverão ser executadas?
Seleccione as tarefas adicionais que deseja que o Assistente de Instalação execute na instalação do Firebird e em seguida clique em Seguinte.
Usar o Guardian para controlar o servidor?
Executar o servidor Firebird como:
Executar como Aplicação?
Executar como um Serviço?
Iniciar o Firebird automaticamente de cada vez que o sistema arranca?
"Instalar a aplicação do Painel de Controlo?"
Copiar a biblioteca do cliente Firebird para a pasta de <system>?
Criar a biblioteca cliente como GDS32.DLL para "retro-compatibilidade"?
Português
< Anterior
Seguinte >
Cancelar

Figura 11

16. Clique em “Instalar” na tela “Pronto para Instalar”.

17. Aguarde o processo de instalação na tela “A instalar”.

18. Clique em “Seguinte >” na tela “Informação”.

19. Desmarque a opção “After installation – What Next?” e clique em “Concluir” na tela “Instalação do Firebird concluída”.

20. Clique em “Next >” na tela “Welcome to the VideoCapX control Setup Wizard”, que será exibida.

21. Clique em “Next >” na tela “Select Destination Directory”.

Observação	*Se quiser instalar em algum outro lugar específico, especifique-o no campo editável no centro da tela.*

22. Clique em “Next >” na tela “Select Start Menu Folder”.
23. Clique em “Install” na tela “Ready to Install”.
24. Aguarde até que seja exibida a próxima tela.
25. Clique em “Finish”.
26. Aguarde o processamento feito durante a exibição da tela “Preparing to Install”.
27. Clique em “Next >” na tela “Welcome to the InstallShield Wizard for VIRDI FP Reader Drivers Ver 2.0”.
28. Aguarde o processamento realizado na tela “Setup Status”.

Observações	*1. Se, em algum momento, for exibida a mensagem “O Windows não pode verificar o editor deste software de driver”, clique em “Instalar este software de driver mesmo assim” quantas vezes forem necessárias.* *2. Se for exibida a mensagem “Deseja instalar este software de dispositivo?”, clique em “Instalar” quantas vezes forem necessárias.*

29. Clique em “Finish” na tela “InstallShield Wizard Complete”.
30. Aguarde a finalização geral da instalação na tela “Instalando”.
31. Clique em “Concluir” na tela “Finalizando o Assistente de Instalação de ZigLock TCP” para encerrar o processo de instalação do *ZigLock TCP Explorer*.

A instalação do *ZigLock TCP Explorer* contempla também os *drivers* necessários para a utilização do *Hamster ZigLock*, responsável pela coleta das impressões digitais dos usuários.

ATENÇÃO	*1. Se você utiliza o Windows 7, após a conclusão da instalação, vá até a área de trabalho, clique com o botão direito sobre o ícone do ZigLock TCP Explorer (ZigLock TCP), clique em “Propriedades” e em “Avançados...” (aba “Atalho”); então marque a opção “Executar como administrador” e clique em “OK”. Use sempre o atalho da área de trabalho para executar o ZigLock TCP Explorer.* *2. Se você utiliza outra versão do Windows, garanta que o ZigLock TCP Explorer seja executado sempre como administrador para que tudo funcione corretamente.*

Passo 2 – Cadastrando os Pontos de Acesso

Neste ponto, faremos a configuração dos pontos de acesso (catracas e controladores de acesso) do sistema.

É necessário possuir o endereço IP e a porta de rede configurada para cada dispositivo.

Para visualizar e/ou configurar a comunicação TCP/IP do equipamento, acesse o menu “Config. TCP/IP” utilizando o teclado do próprio equipamento.

Especialmente no caso de haver vários pontos de acesso na rede, é útil deixar anotada a combinação do endereço IP, porta de rede e a sua respectiva localização, a fim de facilitar o cadastro.

Exemplificando:

Ponto de Acesso	Endereço IP	Porta de Rede
Catraca da Recepção	192.168.0.122	1001
Controlador da Engenharia	192.168.0.123	1001

Com esta lista feita, execute novamente o *ZigLock TCP Explorer*; será solicitado o cadastro da empresa; clique em “Sim” para aceitar e em “Cadastrar Pontos de Acesso” na tela de cadastro de empresas.

Observação	*Caso a empresa já tenha sido cadastrada previamente, acesse a função “Cadastros > Pontos de Acesso ZigLock TCP” para abrir o cadastro dos pontos de acesso.*

Quando a tela de cadastro de pontos de acesso for exibida (**Figura 12**), clique em “Novo” e preencha corretamente o “Endereço IP”, a “Porta” e a “Descrição”. Como descrição, utilize uma identificação significativa para o ponto de acesso (exemplo: “Controlador da Engenharia”). O software usará esta descrição fornecida para se referir ao ponto de acesso posteriormente em outros recursos.

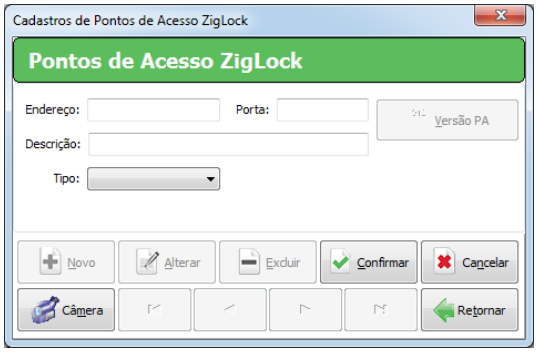


Figura 12

Na sequência, basta selecionar o “Tipo” do ponto de acesso:

- Selecione “Controlador” para especificar um *Controlador ZigLock TCP*.
- Selecione “Catraca” para selecionar uma *Catraca ZigLock TCP*. Neste caso, é necessário também indicar, no campo “Função”, o que será possível controlar nesta catraca: entrada, saída ou entrada/saída (padrão). Também é necessário indicar, ao software, em qual sentido (horário/anti-horário) está associada a entrada ou a saída, de maneira que a catraca consiga controlar corretamente o acesso dos usuários.

ATENÇÃO	*É importante a catraca estar ligada quando esta configuração for cadastrada (primeira vez) ou alterada (próximas vezes), pois ela receberá, do PC, a configuração selecionada logo após o pressionamento do botão “Confirmar”.*

Finalizando, é possível também associar uma câmera para a captura de imagens dos usuários no momento da tentativa de acesso. Isto é possível através do botão “Câmeras”. Clicando neste botão, será aberta a tela “Associação de Câmeras aos Pontos de Acesso” (**Figura 13**). Selecione a câmera desejada para o respectivo ponto de acesso e clique em “Confirmar”.

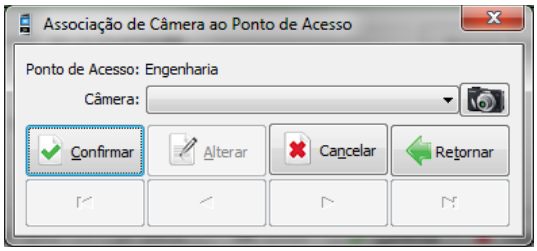


Figura 13

De volta à tela de cadastro de pontos de acesso (**Figura 12**), clique em “Confirmar” para finalizar o cadastro.

Passo 3 – Cadastrando uma Empresa

Na sequência, é necessário cadastrar, pelo menos, uma empresa e associar os pontos de acesso recentemente cadastrados no **Passo 2 – Cadastrando os Pontos de Acesso**. Isto fará com que, no momento do cadastro de um novo usuário, sejam mostrados somente os pontos de acesso da empresa selecionada ao usuário, facilitando o cadastro.

Se a janela de cadastro de empresas já não estiver aberta (do passo anterior), selecione o menu “Cadastros > Empresas” para abri-la (**Figura 14**).

Figura 14

O único campo de digitação obrigatória é a “Razão Social”.

No campo “Pontos de Acesso Associados à Empresa”, aparecem todos os pontos de acesso previamente cadastrados. Porém, é possível, também, acessar o cadastro dos pontos de acesso clicando em “Cadastrar Pontos de Acesso”.

Em “Pontos de Acesso Associados à Empresa”, selecione os pontos de acesso que sejam relacionados à empresa que está sendo cadastrada.

Finalize o cadastro de empresas clicando em “Confirmar”.

Passo 4 – Cadastrando um Usuário

Uma vez com os pontos de acesso e a empresa cadastrados, podemos cadastrar um novo usuário. Este recurso é acessível pelo menu “Cadastros > Usuários”.

Já na tela, conforme **Figura 15**, inicie o cadastro clicando em “Novo”.

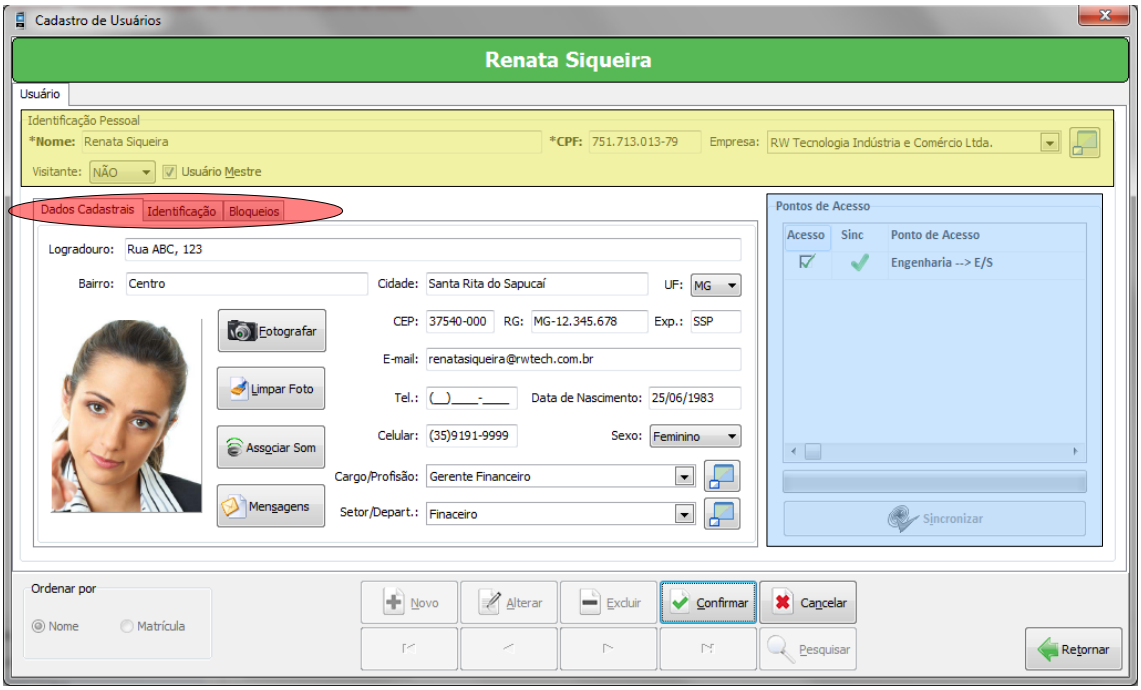


Figura 15

Entre com os dados a seguir, como pode ser visto na **Figura 15:**

- Nome: nome do usuário.
- CPF: CPF do usuário.
- Empresa: empresa atrelada ao usuário, para que os pontos de acesso, relacionados à empresa, sejam disponibilizados ao usuário em “Pontos de Acesso” (em azul, na **Figura 15**).
- Pontos de Acesso: pontos de acesso relacionados à empresa selecionada. Para que o usuário tenha, de fato, acesso controlado num determinado dispositivo, é necessário selecionar o item “Acesso” relativo ao ponto de acesso. Os pontos de acesso não selecionados, bloquearão, incondicionalmente, o usuário (inclusive se estiver marcado como mestre), pois eles simplesmente não reconhecerão o usuário (o cadastro não é enviado para os pontos de acesso não selecionados ou é enviada a exclusão do usuário, se seu cadastro já estiver lá).
- Visitante: sinalização de que o usuário é ou não um visitante. Ao sinalizar que o usuário, SIM, é um visitante, o software muda para a aba “Bloqueios” (vermelho, na **Figura 15**), solicitando o preenchimento do campo “Motivo da Visita” (obrigatório) e sugerindo um possível bloqueio por período de data (opcional).

Observação	*O detalhamento dos bloqueios está mais adiante.*

- Usuário Mestre: sinalização de que o usuário é ou não um usuário mestre. Se o usuário for selecionado como mestre, ele possuirá acesso irrestrito, a todo o momento, nos pontos de acessos selecionados (em azul, na **Figura 15**), independente de qualquer bloqueio (aba “Bloqueios”) que possa existir para o usuário.

ATENÇÃO	*A função “Usuário Mestre” deve ser utilizada com o devido cuidado, pois pode implicar em duas situações:* *1. Possíveis problemas de segurança, caso o usuário tenha um cartão de*

	proximidade e este seja indevidamente utilizado por uma pessoa não autorizada. 2. *Necessidade da devida identificação (com matrícula e senha) de um usuário mestre para acessar o menu (tecla "M") do ponto de acesso.*

– Campos opcionais:

  – Foto: foto para a identificação visual do usuário. Com esse recurso, é possível selecionar uma foto gravada no PC (clicando no espaço destinado à foto) ou tirar uma foto instantânea, caso haja uma câmera conectada ao PC (clicando no botão "Fotografar").
  – Som: efeito sonoro para identificar a tentativa de acesso do usuário. Com este recurso, é possível que o software reproduza um arquivo de áudio no momento da tentativa de acesso do usuário, bastando que o usuário selecione o arquivo através do botão "Associar Som".
  – Mensagens: mensagens a serem enviadas dependendo da tentativa e realização de acesso pelo usuário. Para mais informações, vide **Passo 6 – Mensagens de Texto (E-mail e SMS),** na página **30.**
  – Logradouro, Bairro, Cidade, UF, CEP, RG, Exp., E-mail, Tel., Celular, Data de Nascimento, Sexo, Cargo/Profissão e Setor/Depart.: informações específicas a respeito do usuário.

O próximo passo é cadastrar a "Identificação" do usuário (mude para esta aba, indicada em vermelho, na **Figura 15**).

Existem três tipos possíveis de identificação para o usuário:

1. Teclado do ponto de acesso: caso desejado, basta preencher o campo "Senha". A matrícula é preenchida automaticamente. Assim, o usuário terá acesso, no respectivo ponto de acesso, digitando no teclado do equipamento:
   1. Sua matrícula.
   2. Tecla "OK".
   3. Sua senha.
   4. Tecla "OK" novamente.

Observação	*Para sinalizar a ocorrência de pânico para o sistema, basta preencher a senha com um dígito qualquer a mais no final (exemplo: se minha senha é 123, digitando 1234 eu solicito o acesso da mesma forma, porém sinalizando a ocorrência do pânico ao sistema).*

2. Impressão digital: caso seja desejado este método de acesso, clique em "Cadastrar/Editar Digitais" e prossiga selecionando o que deseja. Durante esse processo, será possível: (1) utilizar o "Hamster" ou um "Ponto de Acesso" para a captura e adição de novas digitais, (2) excluir determinadas digitais e (3) escolher qual digital será utilizada para sinalizar pânico para o sistema.

Observação	*Durante o cadastro de uma nova digital, fique atento às orientações que serão exibidas na tela do PC ou no próprio ponto de acesso selecionado. Caso queira limpar todas as digitais cadastradas para o usuário, clique em "Excluir Todas Digitais".*

3. Cartão de proximidade: caso desejado, preencha este campo com o valor do cartão, que pode ocorrer de duas maneiras:

   1. Leitura e entrada manuais dos números do cartão (no exemplo da **Figura 16**, o número "0073831410" deve ser digitado no campo "Cartão", sendo que o preenchimento dos zeros à esquerda é opcional).

Figura 16

2. Leitura automática dos números do cartão através do *Cadastrador de Cartões ZigLock*, bastando clicar no campo “Cartão” e aproximar dele o cartão a ser cadastrado.

Uma vez finalizado o cadastro do usuário, deve-se clicar em “Confirmar”. Neste momento, o software solicita a autorização do usuário e (se autorizado) envia, aos pontos de acesso selecionados, todas as informações referentes ao usuário, incluindo: nome, CPF, bloqueios e identificadores (incluindo as impressões digitais normais e de pânico). Neste momento, os pontos de acesso devem estar acessíveis na rede para que o envio seja realizado com sucesso.

Como pode ser visto na **Figura 17**, é possível verificar o *status* do envio do usuário para cada ponto de acesso. Na situação normal (todos os pontos de acesso da rede presentes e ligados), todos são atualizados automaticamente com a informação do novo usuário cadastrado. Caso não haja sucesso na atualização do usuário em um ponto de acesso, o ícone “Sinc” aparece com um ponto de exclamação. Para estes casos, existe o botão “Sincronizar” para fazer uma nova tentativa de atualização dos pontos de acesso.

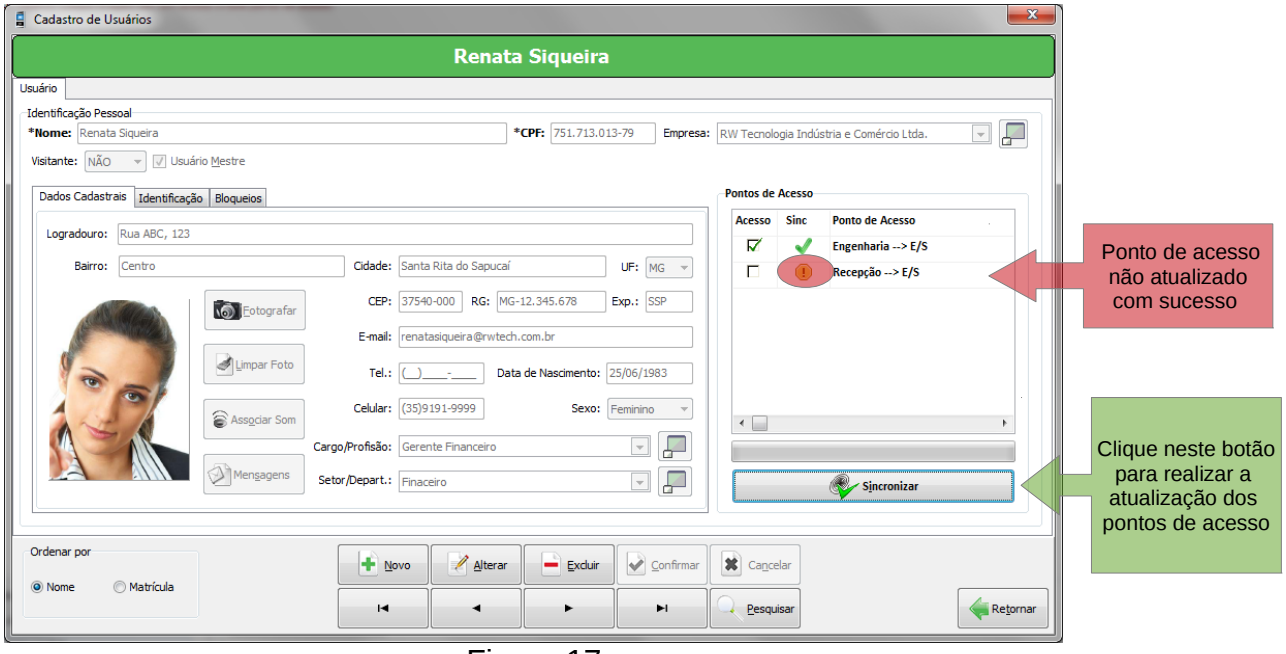


Figura 17

Desta forma, a partir deste momento, o usuário está apto a se identificar no equipamento, estando o PC ligado ou não.

Para cada tentativa de acesso dos usuários (bem-sucedida ou não), será gerado um *Evento de Acesso*, que é mostrado através da tela inicial do software (**Figura 18**),

sendo possível, também, verificar se os pontos de acesso estão visíveis na rede (*online*), bem como realizar esta busca (botão *Atualizar Status*).

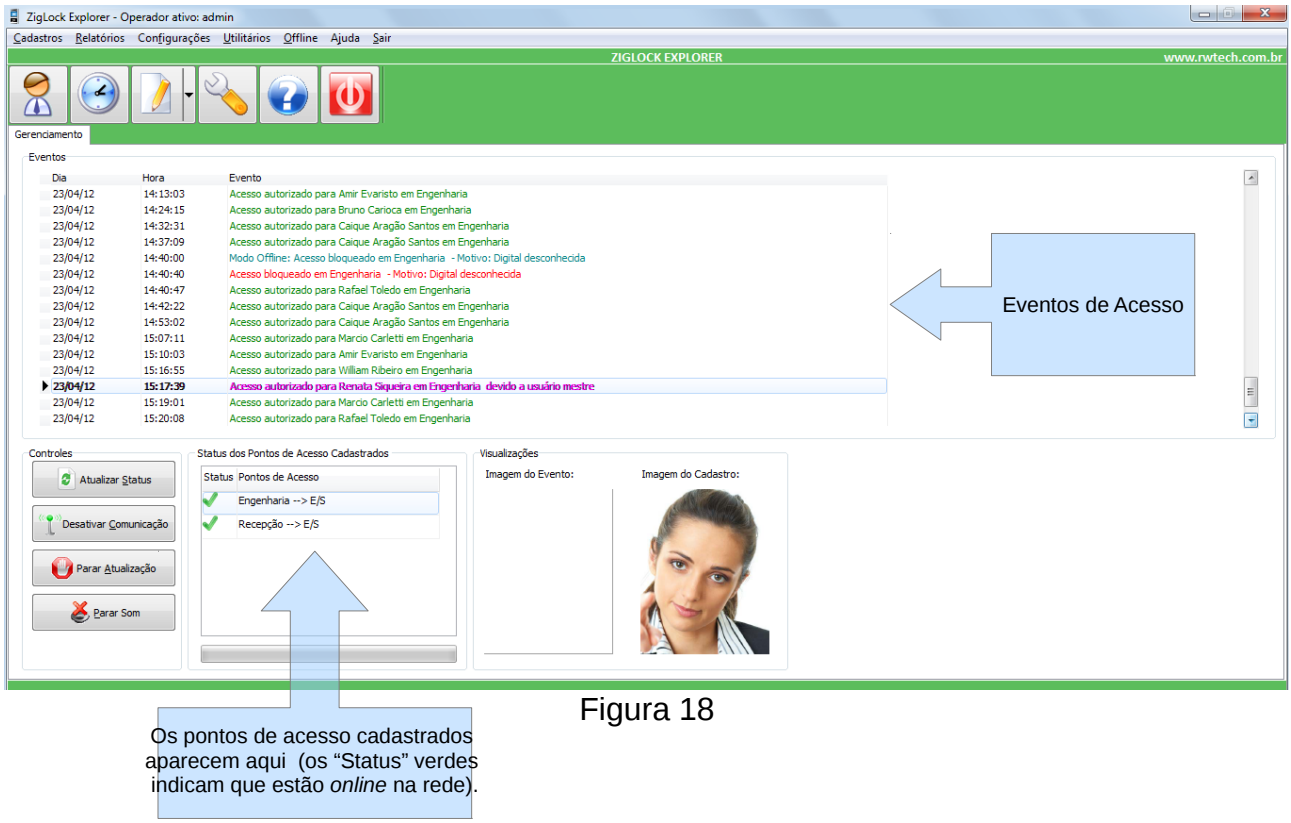

ZigLock Explorer - Operador ativo: admin
Cadastros Relatórios Configurações Utilitários Offline Ajuda Sair
ZIGLOCK EXPLORER
www.rwtech.com.br
Gerenciamento
Eventos
Dia Hora Evento
23/04/12 14:13:03 Acesso autorizado para Amir Evaristo em Engenharia
23/04/12 14:24:15 Acesso autorizado para Bruno Carioca em Engenharia
23/04/12 14:32:31 Acesso autorizado para Caique Aragão Santos em Engenharia
23/04/12 14:37:09 Acesso autorizado para Caique Aragão Santos em Engenharia
23/04/12 14:40:00 Modo Offline: Acesso bloqueado em Engenharia - Motivo: Digital desconhecida
23/04/12 14:40:40 Acesso bloqueado em Engenharia - Motivo: Digital desconhecida
23/04/12 14:40:47 Acesso autorizado para Rafael Toledo em Engenharia
23/04/12 14:42:22 Acesso autorizado para Caique Aragão Santos em Engenharia
23/04/12 14:53:02 Acesso autorizado para Caique Aragão Santos em Engenharia
23/04/12 15:07:11 Acesso autorizado para Marcio Carletti em Engenharia
23/04/12 15:10:03 Acesso autorizado para Amir Evaristo em Engenharia
23/04/12 15:16:55 Acesso autorizado para William Ribeiro em Engenharia
23/04/12 15:17:39 Acesso autorizado para Renata Siqueira em Engenharia devido a usuário mestre
23/04/12 15:19:01 Acesso autorizado para Marcio Carletti em Engenharia
23/04/12 15:20:08 Acesso autorizado para Rafael Toledo em Engenharia
Eventos de Acesso
Controles
Atualizar Status
Desativar Comunicação
Parar Atualização
Parar Som
Status dos Pontos de Acesso Cadastrados
Status Pontos de Acesso
Engenharia --> E/S
Recepção --> E/S
Visualizações
Imagem do Evento:
Imagem do Cadastro:
Os pontos de acesso cadastrados aparecem aqui (os "Status" verdes indicam que estão *online* na rede).

Figura 18

Observações	*1ª) Quando o relógio do ponto de acesso estiver desajustado, ele será ajustado automaticamente com o horário do PC após a primeira identificação de um usuário reconhecido, seja pela digital, pelo cartão ou pelo teclado.* *2ª) Para garantir que os relógios dos pontos de acesso fiquem sempre ajustados e sincronizados com o relógio do PC, os pontos de acesso realizam, automaticamente, o ajuste de seus próprios relógios nas horas ímpares do dia, solicitando a hora atual para o PC.*

Passo 5 – Cadastrando Bloqueios

Os bloqueios disponíveis para a aplicação aos usuários estão disponíveis na aba "Bloqueios", no cadastro de usuários. Por padrão, todos os bloqueios são desabilitados, devendo ser atribuídos aos usuários conforme a necessidade da empresa para cada um deles.

Durante o cadastro de um novo usuário, basta selecionar (e configurar, se necessário) cada bloqueio (em vermelho na **Figura 19**) desejado ao usuário e clicar em "Confirmar". No caso do usuário já estar cadastrado: (1) ache o cadastro dele, (2) clique em "Alterar", (3) realize a ativação (e configuração, caso necessário) e (4) confirme clicando em "Confirmar".

Após confirmar o cadastro ou a edição do cadastro do usuário, o sistema passará a operar com a nova configuração e os pontos de acesso serão devidamente atualizados (caso o usuário autorize e eles estejam acessíveis na rede), **realizando também esses bloqueios quando *offline***.

Observação	*O usuário somente terá acesso permitido ao ponto de acesso se nenhum dos bloqueios*

	se encaixar ao momento e situação dele. Se um ou mais bloqueios for efetuado ao usuário, ele não poderá acessar o ponto de acesso e receberá a justificativa do bloqueio no display do próprio equipamento.

ATENÇÃO	*Se o usuário estiver selecionado como "Usuário Mestre", nenhum dos bloqueios, mesmo que configurados, será efetuado a ele, ou seja, um usuário mestre possui acesso irrestrito aos pontos de acesso, em que estiver cadastrado, a qualquer dia e momento.*

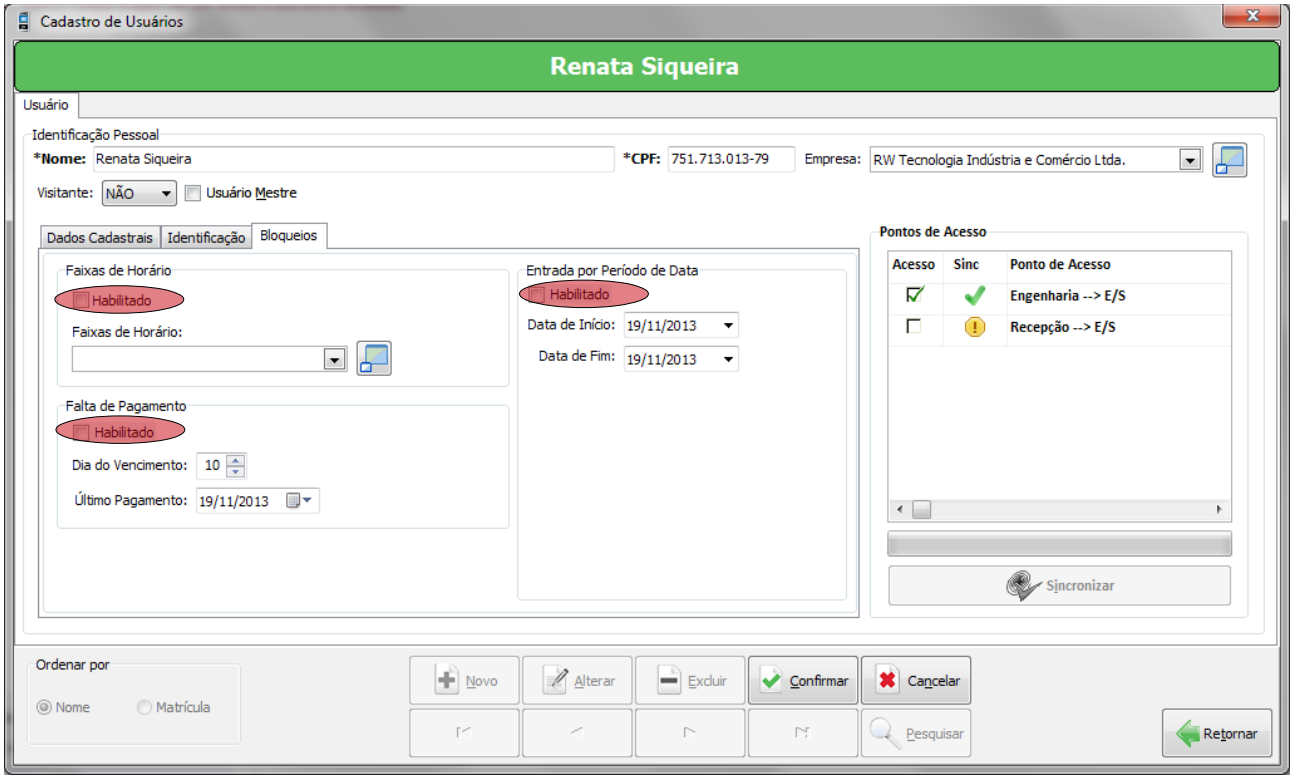


Figura 19

a) Faixas de Horário

Se for habilitada alguma faixa de horário ao usuário, seu acesso será bloqueado em qualquer momento que não esteja dentro dela; o usuário somente poderá ter acesso ao ponto de acesso se ele estiver dentro da faixa de horário configurada **e** não se encaixar em outro bloqueio que esteja habilitado.

O cadastro das faixas de horário pode ser feita sem sair desta tela, clicando no botão da **Figura 20.**

Figura 20

A **Figura 21** mostra a tela de cadastro de faixas de horários. Siga os seguintes passos, observando as indicações de cores na figura, para realizar o cadastro de uma nova faixa de horário:

1. Entre com os horários nos períodos desejados (em amarelo).
2. Entre com um nome para identificar o horário (em azul).
3. Selecione os dias da semana (em vermelho) para os quais se deseja aplicar os

horários digitados no passo 1.

4. Clique em “Aplicar” (em verde).

Observação	*Caso necessário, é possível alterar ou criar um horário para um dia específico da semana, digitando o horário diretamente nas faixas deste dia da semana.*

5. Ao terminar o cadastro, clique em “Confirmar”.

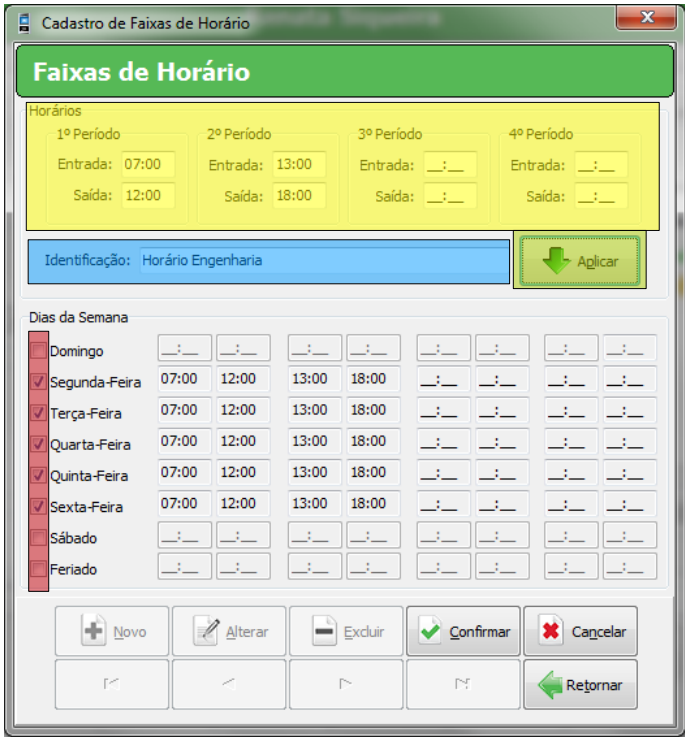


Figura 21

Observação	*Ao selecionar o dia “Feriado” ao cadastrar uma faixa de horário, serão considerados somente os feriados oficiais de vigência nacional, são eles: Confraternização Universal (1º de janeiro), Tiradentes (21 de abril), Dia Mundial do Trabalho (1º de maio), Independência do Brasil (7 de setembro), Nossa Senhora Aparecida (12 de outubro), Finados (2 de novembro), Proclamação da República (15 de novembro) e Natal (25 de dezembro).*

De volta ao cadastro do bloqueio para o usuário, para aplicar a faixa de horário cadastrada ao usuário, basta selecioná-la pelo seu nome e selecionar a opção “Habilitado”.

b) Falta de Pagamento

É útil para clubes, academias e afins, bloquear os usuários caso não seja efetuado um pagamento periódico mensal.

O ponto de acesso passará a bloquear o usuário um dia após marcado no “Dia do Vencimento”, caso o campo “Último Pagamento” não tenha sido realizado no mês corrente. Assim, este campo deve ser atualizado mensalmente, para toda vez que o pagamento for efetuado.

Observação	*Para não constranger o usuário num eventual bloqueio por falta de pagamento, o equipamento exibe a mensagem “**Verifique Suas Pendências!**”, em vez de “Falta de Pagamento!”, por exemplo.*

c) Entrada por Período de Data

Recurso utilizado para restringir o período (entre a data inicial e a data final) no qual o acesso de um determinado usuário é válido. Para o caso do cadastro de visitantes, o campo “Motivo da Visita” é de preenchimento obrigatório.

Passo 6 – Mensagens de Texto (E-mail e SMS)

O *ZigLock TCP Explorer* é capaz de enviar mensagens de texto (e-mail ou SMS), através da internet, nas seguintes condições:

1. Eventos do sistema, como: qualquer acesso bloqueado/autorizado automaticamente, ocorrência de violação do equipamento, ocorrência de pânico, etc.
2. Evento de um usuário específico: acesso liberado/negado para este usuário.

Para o caso do envio de mensagens por SMS, é necessário que o cliente compre créditos com o parceiro *Zenvia*. Esta empresa é especialista neste tipo de serviço, o que garante que as mensagens sejam recebidas nas mais diversas operadoras, além de ser possível acessar relatórios gerenciais dos envios de mensagens. Para mais informações, acesse: *www.zenvia.com.br*.

Uma vez de posse das informações de “Usuário” e “Senha” *Zenvia*, basta configurá-los acessando o menu do *ZigLock TCP Explorer*: “Configurações > Envio de SMS”.

a) Enviando Mensagens de Texto para os Eventos do Sistema

E-mail:

1. Acesse o menu “Configurações > Envio de E-mail”.
2. Clique em “Novo”.
3. Selecione os eventos desejados.
4. Em “Destinatários”, digite o e-mail do destinatário do e-mail.
5. Clique em “Adicionar”. Repetindo-se os passos 4 e 5 (este), é possível incluir mais de um destinatário para o e-mail.
6. Ao terminar o cadastro, clique em “Confirmar”.

SMS:

1. Acesse o Menu “Configurações > Envio de SMS”.
2. Clique em “Alterar”.
3. Assegure que o “Usuário” e a “Senha” *Zenvia* estejam devidamente preenchidos.
4. Clique em “Associar Envio de SMS aos Eventos”.
5. Clique em “Novo”.
6. Selecione os eventos desejados.
7. Em “Destinatários”, entre com o número do telefone (com o DDD).
8. Clique em “Adicionar”. Repetindo-se os passos 7 e 8 (este), é possível incluir mais de um destinatário para o SMS.
9. Ao terminar o cadastro, clique em “Confirmar”.

b) Enviando Mensagens de Texto para os Eventos de um Usuário Específico

Para realizar este envio, siga os passos:

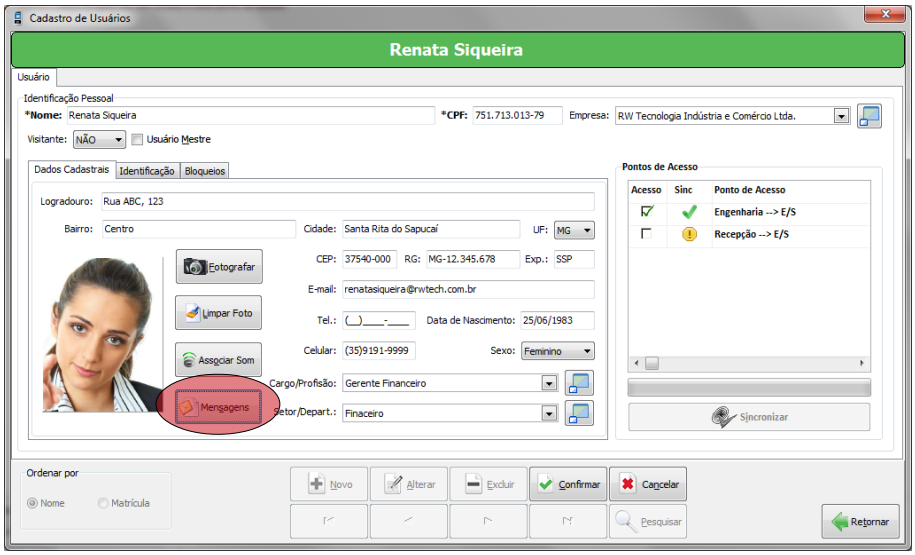


Figura 22

1. Selecione o usuário desejado para aplicar o envio da mensagem de texto.
2. Clique em “Alterar”.
3. Clique em “Mensagens” (vide **Figura 22**).
4. Já na tela da **Erro: Origem da referência não encontrada**, selecione a aba “E-mails” ou “SMSs”, de acordo com o tipo da mensagem desejada.

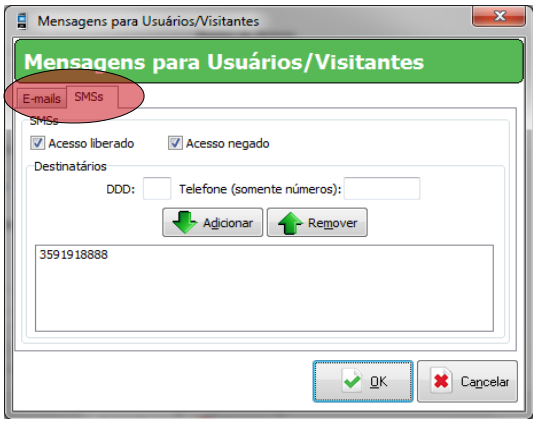


Figura 23

5. Selecione as opções para informar se é desejado o envio quando o usuário tem “Acesso liberado”, “Acesso negado” ou ambos.
6. Digite o número do destinatário do SMS (com o DDD).
7. Clique em “Adicionar”.

Observação	*Repita os passos de 4 a 7 (este) para inserir mais de um destinatário tanto para SMS quando para e-mail.*

8. Clique em “OK” e, depois, em “Confirmar” para finalizar.

Passo 7 – Relatórios

Diversos relatórios gerenciais ou planilhas são disponibilizados pelo sistema, são eles:

a) Relatórios de Acessos

Permitem a escolha de diversos filtros para a exibição dos relatórios ou planilhas,

como: tipo de acesso (negado/autorizado), relatórios por: período, empresa, setor/departamento, cargo/profissão, etc.

b) Usuários por Ponto de Acesso

Lista os usuários cadastrados em um devido ponto de acesso.

Passo 8 – Utilitários

O menu “Utilitários” dá acesso às seguintes funcionalidades:

a) Operadores

O cadastro de um operador permite a restrição do acesso de certas funcionalidades **do software**. Diferentes “visões” do software podem ser criadas, cada qual para um operador diferente.
Para cadastrar um novo operador:

1. Acesse o menu “Utilitários > Operadores > Cadastrar Operadores”.
2. Clique em “Novo”.
3. Digite o nome em “Operador” e a sua “Senha” (que deve ser repetida no campo “Confirmar senha”).
4. Selecione as funcionalidades que devem ser liberadas para o operador.
5. Clique em “Confirmar” para finalizar.

É possível trocar de operador pelo menu “Utilitários > Operadores > Alternar Operador”.

Observação	*Se todos os operadores forem excluídos, o sistema volta à configuração original de não solicitar operador e senha para acesso ao software.*

b) *Backup*

Através do menu “Utilitários > Backup > Criar Backup”, é possível realizar uma cópia de segurança de todos os dados do software. Acessando esta funcionalidade, o sistema gerará um arquivo “.zle” de *backup*. Recomenda-se que este arquivo de *backup* seja salvo em uma mídia removível externa e mantida com segurança.

É possível restaurar um *backup,* criado através do menu “Utilitários > Backup > Restaurar Backup”, apontando para o local onde o arquivo foi salvo.

ATENÇÃO	*A opção de “Restaurar Backup” sobrescreve todas as informações atuais do programa e não pode ser desfeita.*

c) Operações em Massa

Através do menu “Utilitários > Operações em Massa > Sincronização”, é possível realizar o envio (sincronização) de usuários para um ou mais pontos de acesso, evitando ter de abrir cadastro por cadastro para clicar em “Sincronizar”.

d) Visualizar Log

Através desta opção é possível visualizar o log de erros na tela principal do sistema.

Passo 9 –ZigLock em Rede - Modo Servidor / Modo Estação

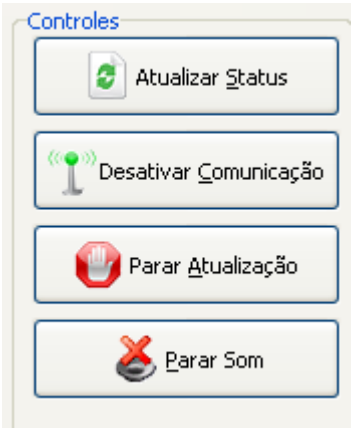
É possível utilizar o ZigLock Explorer em rede (modo estação) para visualização dos eventos, que serão atualizados automaticamente. Os eventos serão mostrados de acordo com a atualização do banco de dados, e neste modo não há comunicação com os pontos de acesso.

Quando for utilizar o ZigLock Explorer em rede, não é recomendável que o sistema operacional do computador designado como "servidor" seja o Windows XP, pois as estações poderão não encontrar o banco de dados. Caso não utilize o sistema em rede, não há restrição com relação ao sistema operacional citado.

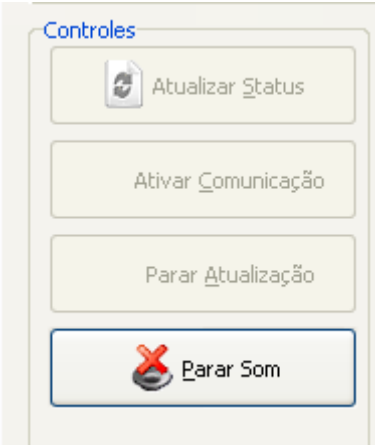
O que define se o ZigLock Explorer será usado como servidor ou estação é um arquivo chamado "localizacao.rwt" (abaixo é descrito como criá-lo). Ao entrar no ZigLock Explorer é verificado se existe o arquivo, se existir, o computador abrirá o sistema em modo estação, caso contrário, abrirá em modo servidor.

Atenção: **Apenas um computador poderá ser usado com Modo Servidor**.

Controles com modo servidor ativado:



Controles com modo estação ativado:



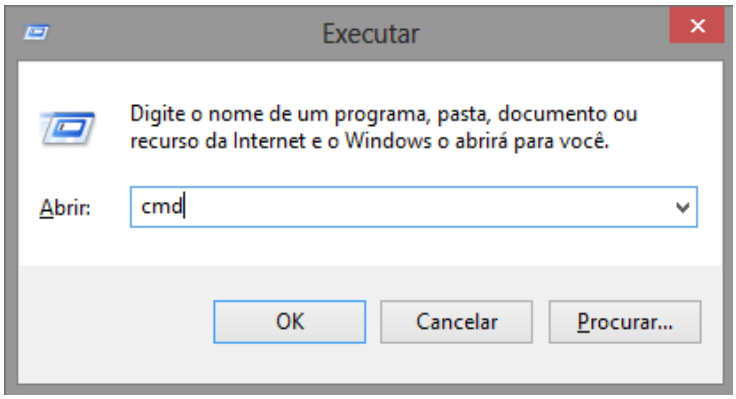
Para colocar o ZigLock Explorer em rede:

*Estação : Computador que acessará o banco de dados do servidor.

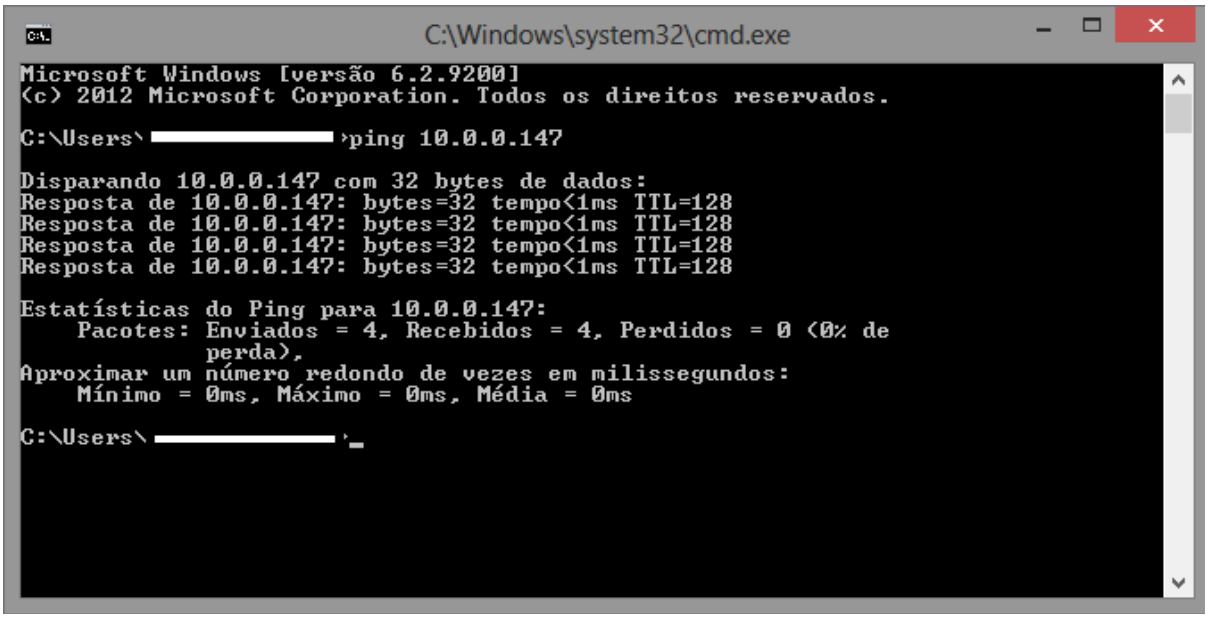
*Servidor: Onde ficará o banco de dados e o *Coordenador ZigLock***.**

Após a instalação do ZigLock Explorer no servidor e nas estações, deve-se seguir os procedimentos abaixo:

Verificar se o IP do servidor está “pingando no estação”. Para isso, execute o cmd.



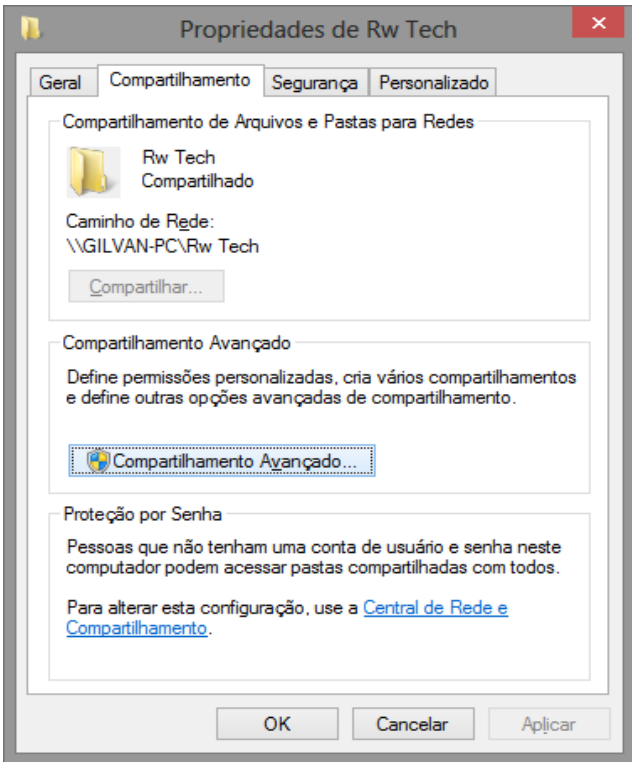
No prompt de comando, digite: ping “ip do servidor”


C:\Windows\system32\cmd.exe
Microsoft Windows [versão 6.2.9200]
(c) 2012 Microsoft Corporation. Todos os direitos reservados.
C:\Users\ ›ping 10.0.0.147
Disparando 10.0.0.147 com 32 bytes de dados:
Resposta de 10.0.0.147: bytes=32 tempo<1ms TTL=128
Resposta de 10.0.0.147: bytes=32 tempo<1ms TTL=128
Resposta de 10.0.0.147: bytes=32 tempo<1ms TTL=128
Resposta de 10.0.0.147: bytes=32 tempo<1ms TTL=128
Estatísticas do Ping para 10.0.0.147:
Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
Mínimo = 0ms, Máximo = 0ms, Média = 0ms
C:\Users\ ›_

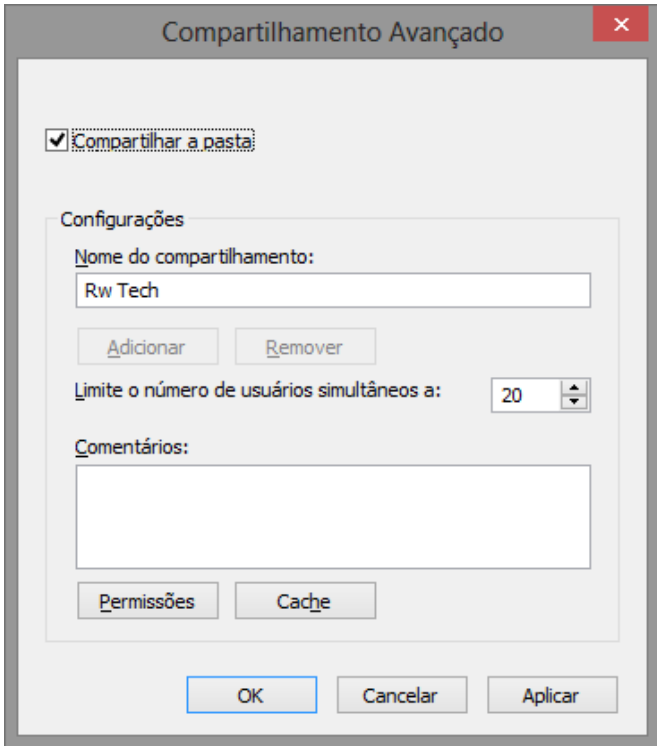
Quando o comando for executado, se aparecer a mensagem de perdidos ou host inacessível, verifique a rede ou entre em contato com o TI da empresa. Caso contrário, continue a executar os passos.

No “SERVIDOR” , na pasta ‘arquivos de programas’, clicar com o botão direito em cima da pasta ‘RwTech’ e em propriedades:

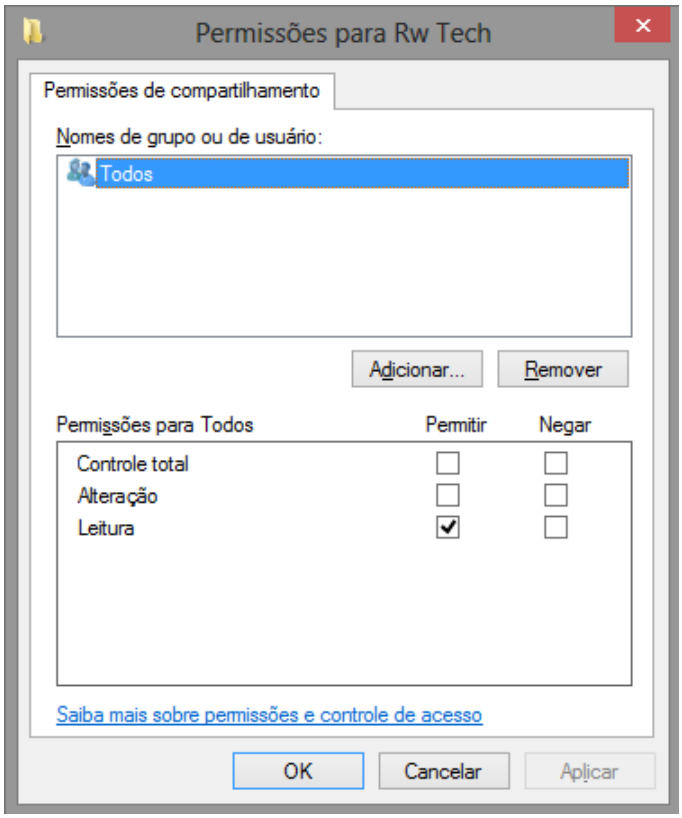
Na aba compartilhamento clicar em ‘compartilhamento avançado’.



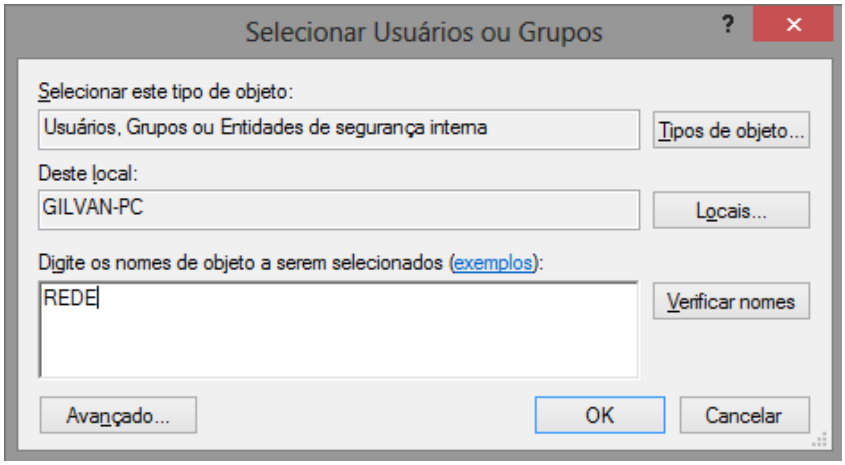
Marcar a opção ‘Compartilhar pasta’, depois em permissões.



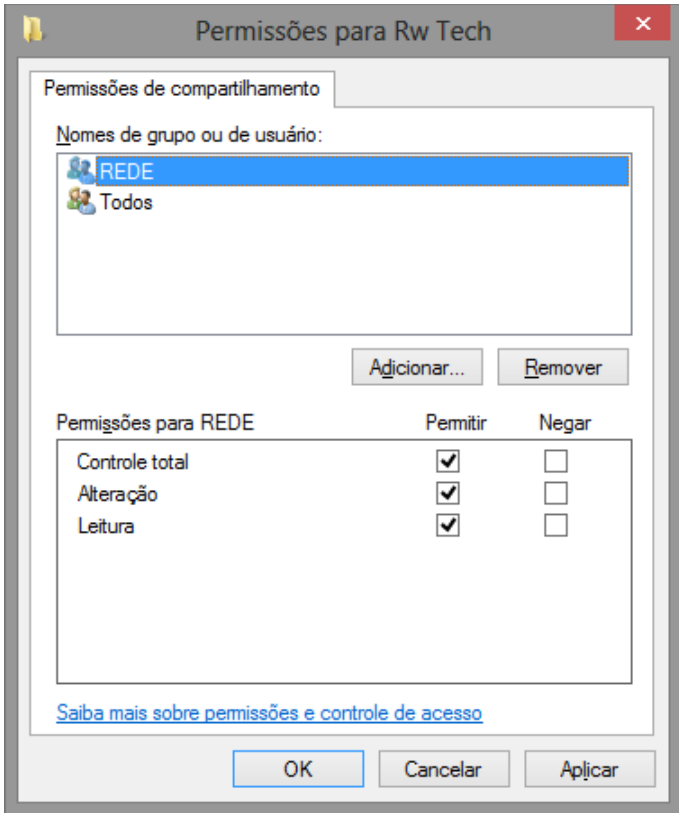
Dentro de permissões clicar em adicionar.

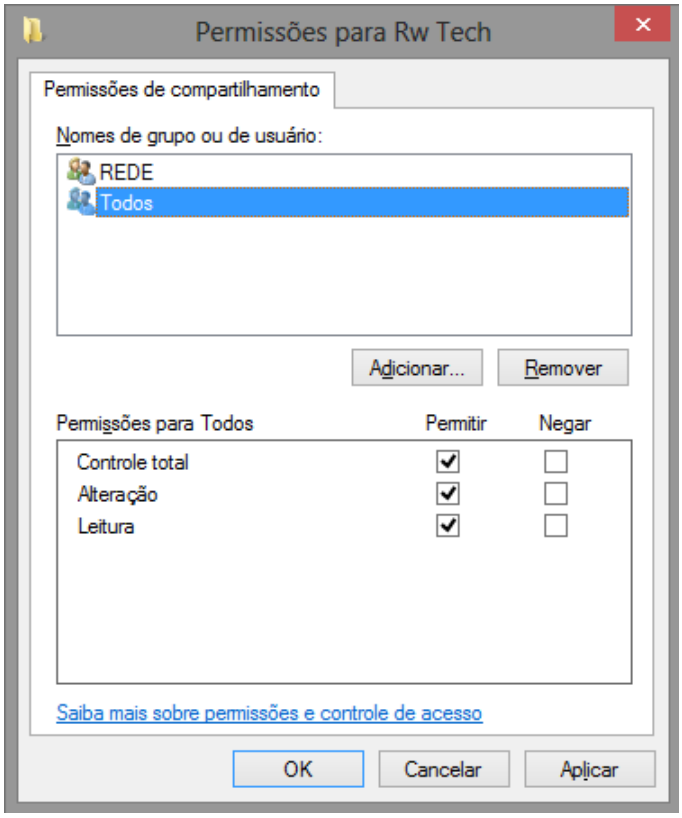


Escrever ‘REDE’ e clicar em ok.

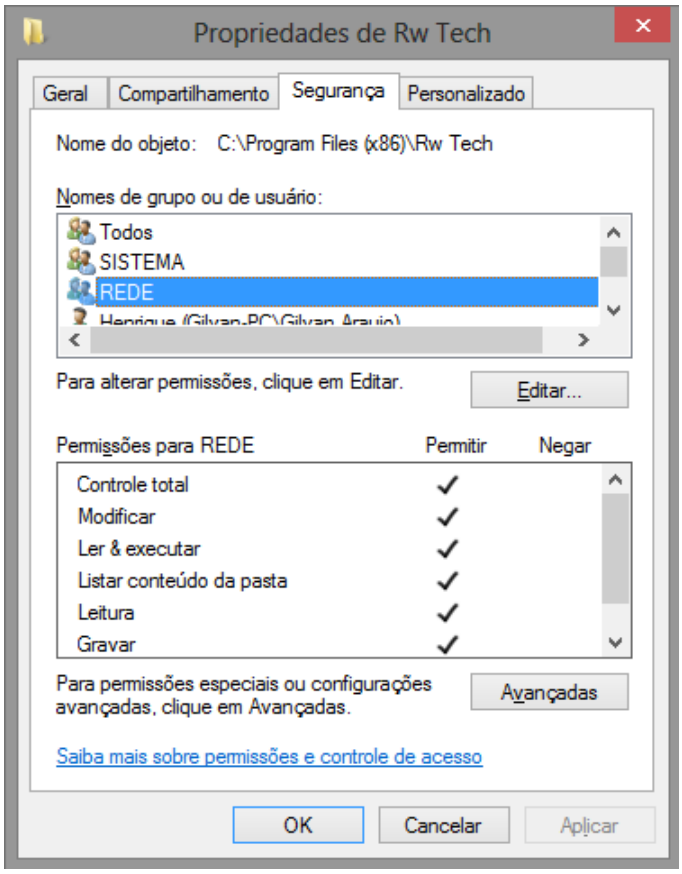


Clicar para dar permissão a todas opções, tanto para rede quanto para todos.

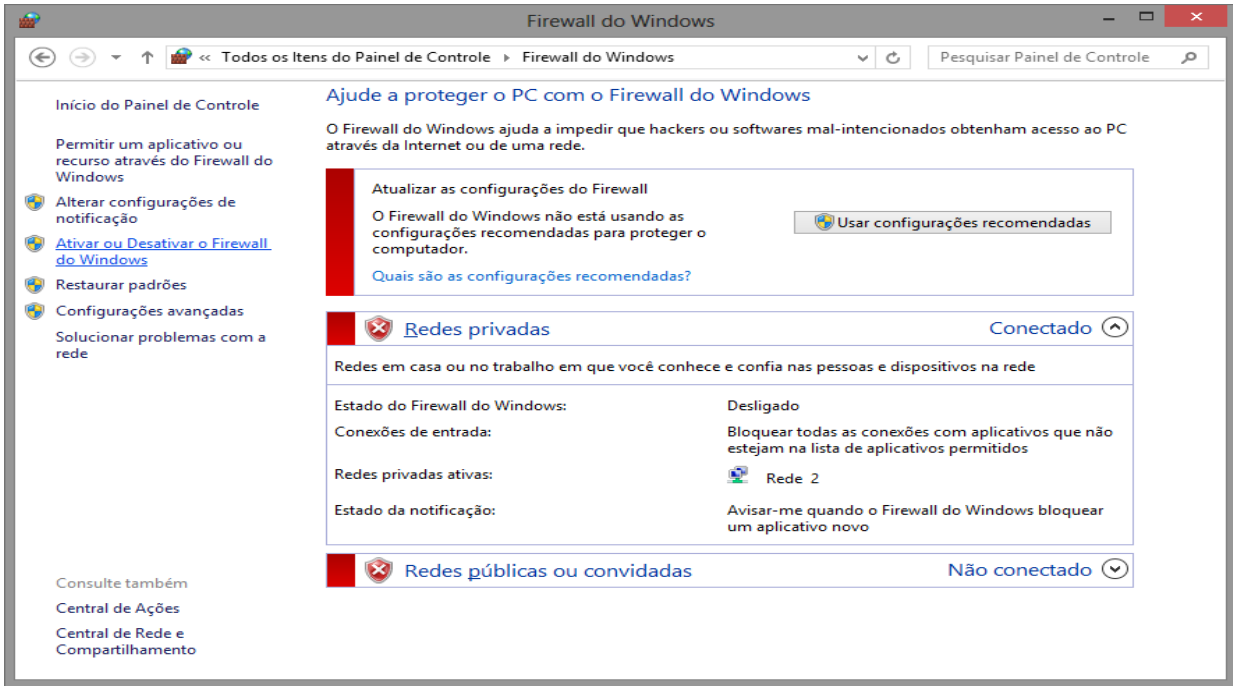




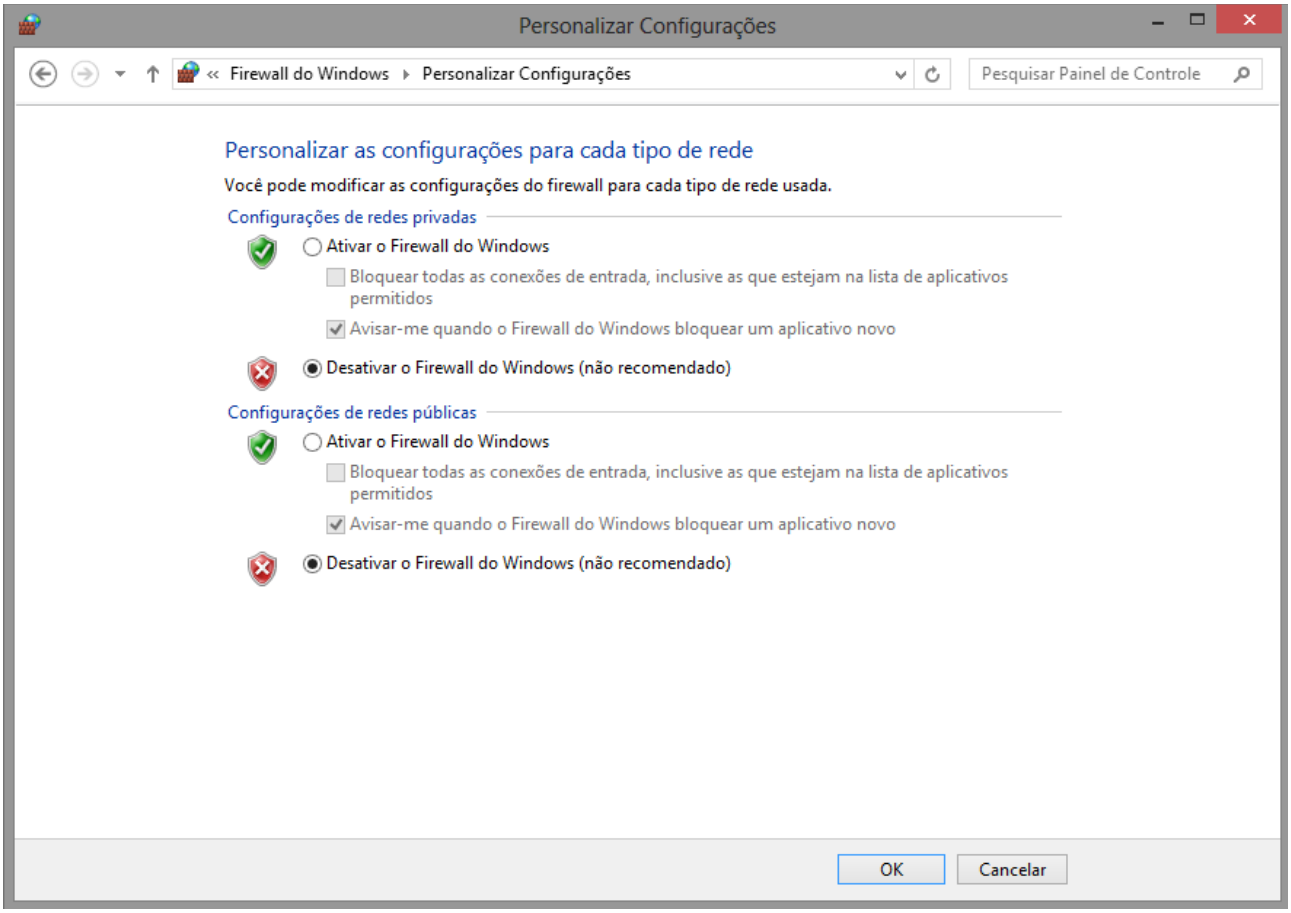
Clicar OK duas vezes, selecionar aba segurança, clicar em editar e repetir o processo anterior, para ter permissão para todos e para rede.



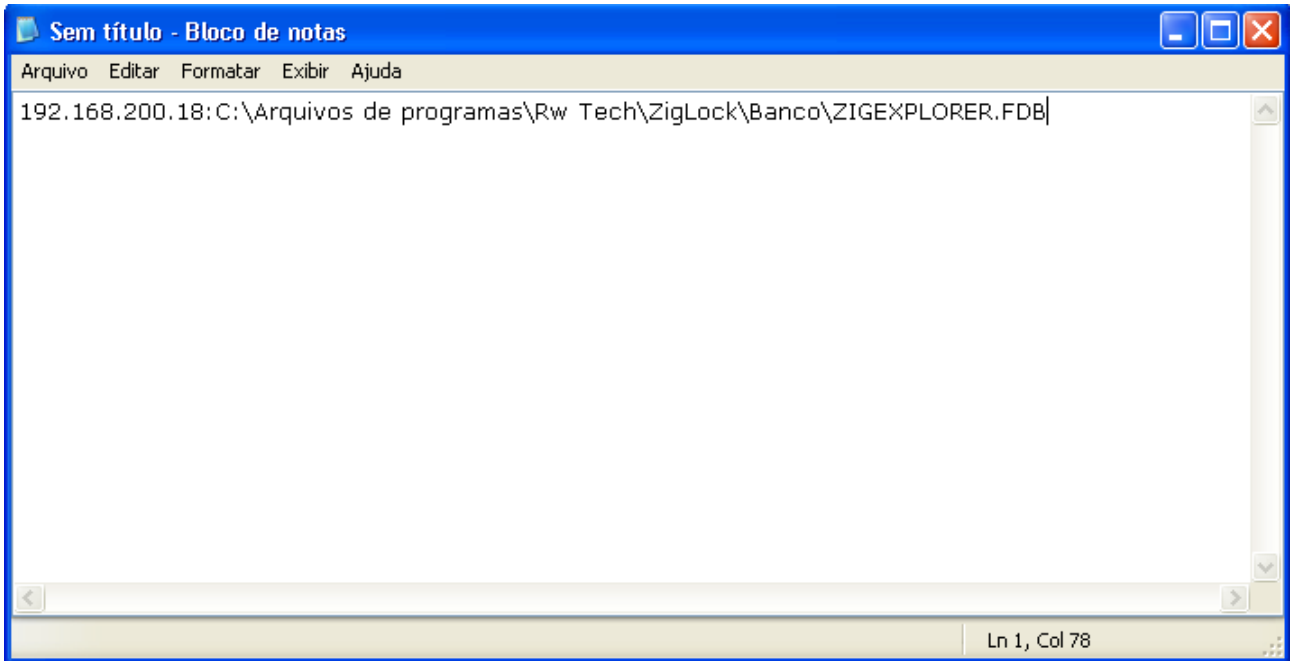
Desativar o Firewall do servidor ou criar uma exceção para a porta 3050 (Firebird);


Firewall do Windows
Todos os Itens do Painel de Controle ▸ Firewall do Windows
Pesquisar Painel de Controle
Início do Painel de Controle
Permitir um aplicativo ou recurso através do Firewall do Windows
Alterar configurações de notificação
Ativar ou Desativar o Firewall do Windows
Restaurar padrões
Configurações avançadas
Solucionar problemas com a rede
Ajude a proteger o PC com o Firewall do Windows
O Firewall do Windows ajuda a impedir que hackers ou softwares mal-intencionados obtenham acesso ao PC através da Internet ou de uma rede.
Atualizar as configurações do Firewall
O Firewall do Windows não está usando as configurações recomendadas para proteger o computador.
Usar configurações recomendadas
Quais são as configurações recomendadas?
Redes privadas
Conectado
Redes em casa ou no trabalho em que você conhece e confia nas pessoas e dispositivos na rede
Estado do Firewall do Windows:
Desligado
Conexões de entrada:
Bloquear todas as conexões com aplicativos que não estejam na lista de aplicativos permitidos
Redes privadas ativas:
Rede 2
Estado da notificação:
Avisar-me quando o Firewall do Windows bloquear um aplicativo novo
Redes públicas ou convidadas
Não conectado
Consulte também
Central de Ações
Central de Rede e Compartilhamento

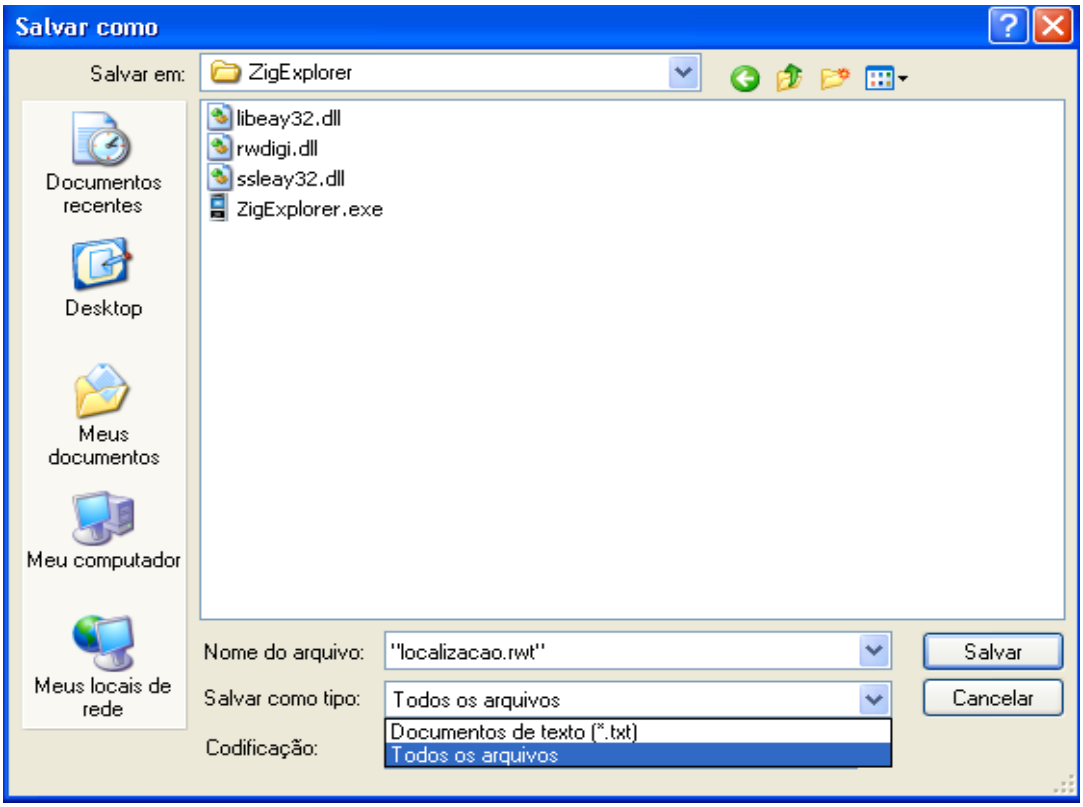
Desativar


Personalizar Configurações
« Firewall do Windows ▸ Personalizar Configurações
Pesquisar Painel de Controle
Personalizar as configurações para cada tipo de rede
Você pode modificar as configurações do firewall para cada tipo de rede usada.
Configurações de redes privadas
Ativar o Firewall do Windows
Bloquear todas as conexões de entrada, inclusive as que estejam na lista de aplicativos permitidos
Avisar-me quando o Firewall do Windows bloquear um aplicativo novo
Desativar o Firewall do Windows (não recomendado)
Configurações de redes públicas
Ativar o Firewall do Windows
Bloquear todas as conexões de entrada, inclusive as que estejam na lista de aplicativos permitidos
Avisar-me quando o Firewall do Windows bloquear um aplicativo novo
Desativar o Firewall do Windows (não recomendado)
OK
Cancelar

Criar um bloco de notas na estação porém com IP do servidor e diretório onde está o banco de dados no servidor. Exemplo:
192.168.1.10:C:\Arquivos de programas\Rw Tech\ZigLock\Banco\ZIGEXPLORER.FDB


Sem título - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
192.168.200.18:C:\Arquivos de programas\Rw Tech\ZigLock\Banco\ZIGEXPLORER.FDB
Ln 1, Col 78

Salvar o bloco de notas como “localizacao.rwt” (colocar aspas) e na opção salvar, salvar como TODOS OS ARQUIVOS;



Colar este bloco de notas na pasta \ZigLock\ZigExplorer das estações. Obs.: Caso esteja tudo de acordo com o tutorial e não esteja rodando em rede, renomear a dll GDS32.dll para _GDS32.dll no servidor.

Notas de Revisão

Rev.	Data	Nota
1.0	17/09/13	- Revisão inicial.
1.1	20/12/13	- Mudança do nome *Human* para *Zenvia*. - Enfatização de que o usuário poderá ser bloqueado mesmo sinalizando pânico. - Atualização necessária para acompanhar o software. - Atualização da especificação das ligações elétricas.
1.2	31/01/14	- Inclusão dos modelos de 480 e 1500 digitais do controlador. - Correção da informação a respeito da fonte de alimentação.
1.3	27/08/14	- Exclusão dos modelos de Coordenador
1.4	04/09/14	- Geração de planilhas - Funcionamento do ZigLock Explorer em rede, para consulta de eventos

GARANTIA

Assegura-se ao *Controlador de Acesso ZigLock TCP* (modelos: *Controlador ZigLock TCP CARD*, *Controlador ZigLock TCP BIOCARD, Catraca ZigLock TCP CARD, Catraca ZigLock TCP BIOCARD 480 e Catraca ZigLock TCP BIOCARD 1500*), *a* garantia contra qualquer defeito de material de fabricação que nele se apresente no período de 1 (um) ano, contados a partir da data de emissão da nota fiscal.

A garantia tornar-se-á nula e sem efeito se o produto sofrer (1) qualquer dano provocado por acidentes, agentes da natureza, desgaste natural das peças e componentes, (2) uso abusivo ou em desacordo com as instruções do manual, (3) descuido do usuário no manuseio, transporte ou remoção do aparelho, ou ainda, (4) no caso de apresentar sinais de violação, ajuste ou conserto por pessoas não autorizadas.

A garantia oferecida limita-se ao conserto ou troca do produto adquirido. A RW Tecnologia não se responsabiliza por possíveis danos causados por incidentes, má-fé ou inabilidade no uso do produto.

RW Tecnologia Indústria e Comércio Ltda.
Enterplak Produtos Eletrônicos Ltda.